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	Stella-Jones Inc. (Organization)
Decision number (file number)	P2021-ND-293 (File #020716)
Date notice received by OIPC	April 19, 2021
Date Organization last provided information	October 13, 2021
Date of decision	March 2, 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 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 incident involved some or all of the following information: : • name, • address, • date of birth, • social insurance number, • banking information, and • personal health care number. This information is about an 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 13, 2021, an employee with the Organization received a phishing email and did not realize it was not from a trusted source.

	• The employee provided their username and password as well as multi-factor authentication code. • The hacker then logged into the employee's email and address book for several hours. • The Organization reported, "There is no log showing the hacker copied this information, however he had access to it." • The hacker sent emails posing as a senior director of the Organization to external and internal contacts found in the employee's email account. Attachments to the emails requested username and password. • The breach was discovered on April 14, 2021 when several external contacts reported that they received phishing emails from the Organization. • The incident ended on April 14, 2021.
Affected individuals	The incident affected 26 individuals whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Notified the Organization's IT and immediately changed the employee's password and started a detailed analysis of the incident. • Set up a secure portal for all Human Resources matters within the Organization. • Requested employees review their email and repositories for sensitive information, send to HR and permanently delete the data from their Office 365 account. • Will provide cybersecurity training to all employees that use company's information technology tools. • Provided credit monitoring free for 2 years to all affected individuals.
Steps taken to notify individuals of the incident	The affected individuals were notified by letter on April 20, 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 the possible harms that may occur as a result of the breach are, "Fraudulent credit application, identity theft." In my view, a reasonable person would consider that the contact, identity and financial information at issue could be used to cause the significant harms of identity theft, fraud and financial loss.

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 the likelihood that the harm will result as "medium". In my view, a reasonable person would consider that 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 into an employee's email account) who accessed and used the personal information for additional phishing/smishing purposes.

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 significant harms of identity theft, fraud and financial loss. 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 into an employee's email account) who accessed and used the personal information for additional phishing/smishing purposes.

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 letter on April 20, 2021, accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner