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	Sagium Corporation (Organization)
Decision number (file number)	P2022-ND-080(File #023259)
Date notice received by OIPC	September 29, 2021
Date Organization last provided information	September 29, 2021
Date of decision	January 10, 2023
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: • email address. This information is about an identifiable individual 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 June 25, 2021, the Organization discovered that an unauthorized third party had gained access to its email account using a phishing email that harvested the user's credentials. • For a limited time, the third party was able to view emails that the account had sent. • The forensic firm hired to investigate the incident did not identify evidence of data access or exfiltration within its network beyond any attachments included within the compromised email account.

Affected individuals	The incident affected one (1) individual in Alberta.
Steps taken to reduce risk of harm to individuals	• Immediately disabled its compromised account and contacted a forensic firm to investigate. • Contacted a forensic firm to examine logs, examined available authentication logs and did not identify any malicious activity in the investigated account. • Continuing to implement a two-factor authentication for its email accounts.
Steps taken to notify individuals of the incident	The affected individual was notified by email on September 28, 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 unauthorized access of a client's email address may have led to a potential loss of confidence in Sagium's ability to protect personal information.* In my view, a reasonable person would consider that the email address could be used for the purposes of phishing, increasing the affected individual's 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 assessed the likelihood that the harm will result is "*Possible, but unlikely*". 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 employees' email account). The Organization reported an unauthorized access of personal information by a third party who was able to view emails that the account had sent.
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. The email address could be used for the purposes of phishing, increasing the affected individual's vulnerability to identity theft and fraud. These are all significant harms. 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	

employees' email account). The Organization reported an unauthorized access of personal information by a third party who was able to view emails that the account had sent.

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 by email on September 28, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance