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	Law Society of Alberta (Organization)
Decision number (file number)	P2020-ND-140 (File #015953)
Date notice received by OIPC	June 2, 2020
Date Organization last provided information	June 2, 2020
Date of decision	November 3, 2020
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 email addresses, including, possibly, individual names. This is information about identifiable individuals 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 March 18, 2020, the email account of an employee of the Organization was hacked and several hundred phishing emails were sent from the account to Organization staff and to approximately 700 external recipients. • The email purported to send out documents from the employee and requested recipients enter their credentials.

	• The Organization immediately discovered the incident and quarantined the employee's laptop, reset the credentials, searched the system for the messages and deleted all internal messages with a soft delete. Within minutes, an email was sent to all staff to not open the email. • The Organization reported that a review shows that no other users with the Organization were compromised; however, one member of the Organization opened the email and his account was hacked sending out dozens of phishing emails.
Affected individuals	The incident affected approximately 800 individuals.
Steps taken to reduce risk of harm to individuals	• Immediately disabled the account. • Quarantined the computer. • Reset passwords on the account. • Installed two-factor authentication. • Added an external email notification banner on new email. • Tightened network access. • Coordinated activities with security consultants. • Reviewed home computer security. • Upgraded remote access service. • Began security awareness training. • Sent intranet advisories and email communications to all staff regarding cyber security precautions and alerts. • Planning future security measures.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on March 18 and March 23, 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 "As a result of the phishing email – if the recipients entered their credentials, then these is a possibility their system may have been compromised. Because of the quick containment, there are no indications of other personal information being compromised. Since the incident and the notices were sent out, we have only received information from one member …who stated that because he opened the email in question, his account was hacked and that his account sent out several dozen phishing emails...". In my view, a reasonable person would consider that email addresses could be used for the purposes of phishing, 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 "Quick action has resulted in no likelihood of harm." In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because the email addresses were compromised due to the malicious action of an unknown third party (phishing). The lack of reported incidents resulting from this incident is not a mitigating factor, as phishing, identity theft and fraud can occur months and even years after a data breach. Further, the information has already been used for fraudulent 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 email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are significant harms. The likelihood of harm resulting from this incident is increased because the email addresses were compromised due to the malicious action of an unknown third party (phishing). The lack of reported incidents resulting from this incident is not a mitigating factor, as phishing, identity theft and fraud can occur months and even years after a data breach. Further, the information has already been used for fraudulent purposes.

I require the Organization to notify the affected individuals whose 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 March 18, 2020 and March 23, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner