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	Economical Insurance and its subsidiary, Sonnet Insurance Company (Organization)
Decision number (file number)	P2020-ND-101 (File #017099)
Date notice received by OIPC	August 14, 2020
Date Organization last provided information	September 8, 2020
Date of decision	September 17, 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 all or some of the following information: • name, • job title, • work location, • leader name, • date of birth, • category of short term or long term disability (start date, end date, accommodation date), • telephone number, and • information related to calls to customer call centre. 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 July 8, 2020, an employee received a phishing email from an unknown third party. The email included a hyperlink to a page on which the employee entered their username and password. • On July 20, the credentials were used to access the employee's email account and an internal software program, and to send further phishing emails to employees and addresses in the email account. Five other employees subsequently entered their credentials. • The unauthorized activity was identified on July 21, 2020. An investigation found documents containing the information at issue were accessed.
Affected individuals	The incident affected approximately 300 individuals, including 27 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Required employees to reset their access passwords. • Notified the parties who received phishing emails. • Advised all employees of the incident and reminded them to be vigilant against phishing emails. • Reminded staff of processes for identifying individuals when inbound service requests are received. • Contacted third party benefits administrator to report the incident and encourage caution when verifying identification. • Implementing a new multi-factor authentication process.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on August 27, 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 "The information could potentially be used for identity theft and fraud." I agree with the Organization's assessment. A reasonable person would consider that the contact and identity information at issue could be used to cause the harms of identity theft and fraud. Credentials could be used to compromise other online accounts. 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	The Organization reported: *...there is no indication that the improperly accessed information has been used by an unauthorized party or that the information will be misused, but the fact that the incident was caused by a malicious third party does raise a concern of harm.*

between the incident and the possible harm.	In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (phishing email) by an unknown third party and employee credentials were used to obtain information and to send additional phishing emails. Although the Organization has no indication the accessed information has been or will be misused, the Organization cannot rule out the possibility.

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 and identity information at issue could be used to cause the harms of identity theft and fraud. Credentials could be used to compromise other online accounts. 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) by an unknown third party and employee credentials were used to obtain information and to send additional phishing emails. Although the Organization has no indication the accessed information has been or will be misused, the Organization cannot rule out the possibility.

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 in a letter on August 27, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner