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 Mutual Insurance Company (Organization)
Decision number (file number)	P2020-ND-023 (File #013910)
Date notice received by OIPC	November 19, 2019
Date Organization last provided information	December 5, 2019
Date of decision	March 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 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, • residential address, • email address, • contact information for others insured under the policy, • information about the property loss, • expenses, • receipts, and • photographs. This information is 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 October 14, 2019, an independent insurance claims adjusting firm engaged by the Organization to adjust property claims for its policyholders had a break-in and several computers were stolen from its offices. • The information on the computers was encrypted and protected by passwords. However, the Organization reported that a thief may have had access to the encryption password for one of the computers. • The Organization reported that it has no indication that the theft was for the purposes of accessing personal information, but said that is uncertain of this. • To date, two of the stolen laptops have been recovered, but not the computer with the available password. • The police investigation resulted in an arrest of an individual.
Affected individuals	The incident affected 19 individuals.
Steps taken to reduce risk of harm to individuals	• Reported the incident to law enforcement. • Provided a 24-month subscription to a credit monitoring service free of charge.
Steps taken to notify individuals of the incident	The affected individuals were notified by letter on December 3, 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 "With respect to the risk of harm to the individuals, we believe that the information that could be obtained from the e-mail account is about identifiable individuals. There is a risk that, if accessed, the information could be used in order to attempt identity theft or fraud." In my view, a reasonable person would consider that the contact and insurance 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, "We have received no indication that the information has in fact been accessed by an unauthorized individual or that the information has been misused." In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased as it was the result of malicious intent (break-in and theft). The Organization can only speculate as to the motives of the thief. The computer with the available password has not been recovered. The fact there have been no reported incidents of fraud to date does not mitigate

	against future harm as identity theft and fraud can occur months or even years after an incident.

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 insurance 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 it was the result of malicious intent (break-in and theft). The Organization can only speculate as to the motives of the thief. The computer with the available password has not been recovered. The fact there have been no reported incidents of fraud to date does not mitigate against future harm as identity theft and fraud can occur months or even years after an incident.

I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the affected individuals were notified by letter on December 3, 2019. The Organization is not required to notify the individuals again.

Jill Clayton
Information and Privacy Commissioner