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	Co-operators Group Ltd. (Organization)
Decision number (file number)	P2022-ND-002 (File #022182)
Date notice received by OIPC	July 13, 2021
Date Organization last provided information	February 2, 2022
Date of decision	February 14, 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 those 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 the co-operative holding company for The Co-operators group of companies and is responsible for the personal information in this instance. This breach impacted claimants of the Organization's companies, Co-operators General Insurance Company, Cumis General Insurance Company, COSECO Insurance Company, and Sovereign General Insurance Company. The Organization operates in Alberta and 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, • date of birth, • address, • date of loss, • driver's license number, • medical information (including clinical/diagnosis information, mental or physical condition, symptoms, medical procedures, treatment information, OHIP number, prescription information), • religion, • ethnic origin, • social insurance number,

	• complaint information, • marital status, • mother's maiden name, • passport number, • student identification number, • digital signature, • income information, and • employment information. 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	• One of the Organization's insurance claims vendors suffered a malicious attack. • On March 14, 2021, a rogue actor compromised the email account of an employee of the vendor. Seven separate connections were made to the email account on this date. The exact duration of those connections is unclear at this time. • The rogue actor had the ability to access the email account, but it is unclear to the Organization what was accessed inside the email account or whether anything was exfiltrated. • Phishing emails were sent to other individuals that were made to look like they were sent from the affected employee. • On March 26, 2021, the vendor notified the Organization of the incident. • The root cause of the rogue actor's ability to compromise the email account is unknown at this time. • The Organization reported that each individual entity noted in this report is responsible for the personal information in this breach.
Affected individuals	The incident affected 751 Canadians, including 42 individuals whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	<u>Vendor:</u> • Engaged a cybersecurity firm to investigate. • Identified the nature of the attack and the potential extent of the exposure. • Monitoring the dark web for signs of any data exposed as a result of this incident. Monitoring did not turn up evidence of information being posted.

	• Log tracking of email systems to understand the extent of attacks. • Replaced the compromised computer and changed all passwords. • Implemented two-factor authentication to access email within the company. • Deployed additional security software to detect malicious activity on devices within network. <u>Organization:</u> • Offered two years of credit monitoring protection to help reduce the risk of identity theft or financial loss to those individuals for whom date of birth, driver license number, social insurance number, or passport number were exposed. • Indicated to individuals that they should continue to monitor for any usual activity and notify any appropriate authorities to help protect themselves. • Reviewing vendor agreements to determine if revisions are necessary to mitigate future risks. • Contemplating additional steps as a follow-up to this incident.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on September 29, 2021 and October 18, 2021. For affected individuals for whom litigation was currently ongoing, notification letters were sent to counsel.
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, *These attacks could lead to a risk of significant harm such as humiliation, damage to reputation/relationships, loss of employment or financial loss.* *As we are unsure [sic] the extent of this breach, it is best to consider the rogue actor would have been able to access all information in the employee's inbox and that the risk of harm is high.* I agree with the Organization's assessment. A reasonable person would consider that the contact, identity, medical, employment, insurance, financial and profile information, particularly in combination, could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing, increasing vulnerability to identity theft and fraud.

	The medical and profile information could be used to cause hurt, humiliation, and embarrassment. 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 reported, *A reasonable person would consider the likelihood of harm resulting from this incident is high due to the fact the breach was a result of malicious action from a rogue actor.* 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 (unauthorized access). The Organization reported "there was no indication... personal information was directly accessed or taken as part of this attack." However, phishing emails were sent to affected individuals and the Organization does not know the root cause of the rogue actor's ability to compromise the email account. The email account was exposed for approximately two (2) weeks.

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, medical, employment, insurance, financial and profile information, particularly in combination, could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing, increasing vulnerability to identity theft and fraud. The medical and profile information could be used to cause hurt, humiliation, and embarrassment. 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 (unauthorized access). The Organization reported "there was no indication... personal information was directly accessed or taken as part of this attack." However, phishing emails were sent to affected individuals and the Organization does not know the root cause of the rogue actor's ability to compromise the email account. The email account was exposed for approximately two (2) weeks.

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 affected individuals by letter on September 29, 2021 and October 18, 2021, in accordance with the Regulations. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Information and Privacy Commissioner