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	RBC Life Insurance (Organization)
Decision number (file number)	P2021-ND-283 (File #021616)
Date notice received by OIPC	June 10, 2021
Date Organization last provided information	June 10, 2021
Date of decision	February 22, 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 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, • name of household members, • contact information, • home address, • work address, • date of birth, • medical information, • financial information, • claims information, • "information from publicly available sources collected with claims adjudication", • driver's license, and • social insurance number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization uses third party service providers to "assist … in the adjudication of … insurance claims." • On March 17, 2021, the Organization received a suspicious email from one of its third party suppliers. The suspicious email was reported to the third party on March 19, 2021. • The third party investigated and determined that an employee email account was compromised on or about March 14, 2021. The affected email account contained personal information of the Organization's clients.
Affected individuals	The incident affected 1,193 individuals, including 150 whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• The third party contained the incident on or about March 20, 2021, implemented additional security controls, and retained a vendor to enhance monitoring of accounts and systems for suspicious activity. • Suspended activity with the supplier until investigation concluded. • Performing an additional "Supplier Control Assessment". • Advised internal parties who may have a relationship with the affected third party to be vigilant. • Investigated and determined that no one in the Organization visited a link that was included in the suspicious email. • Verified that security controls categorized the link as malicious and access was blocked. • Implemented measures to monitor affected individuals' bank accounts and financial products. • Offered identity and credit monitoring services. • Provided guidance on avoiding phishing. • Notified other regulatory bodies.
Steps taken to notify individuals of the incident	All but one of the affected individuals were notified by letter between June 10 and 18, 2021. One affected individual was not directly notified of the incident due to an ongoing legal matter.

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 possible harms that might result from the incident as… *Embarassment, [sic.] hurt or humilation [sic.]* *Email phishing or spear-phishing attacks* *ID theft/impersonation* I agree with the Organization's assessment. A reasonable person would consider that the identity, insurance, medical, and financial information at issue could be used to cause the harms of identity theft, fraud, and embarrassment, hurt or humiliation. Contact information, such as email addresses, could be used for the purposes of phishing or spear-phishing, increasing the affected individuals' vulnerability to the above. 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 … *… [estimates] a low likelihood of harm to the impacted individuals. Client monitoring activities to date do not show any indication that the … client personal information has been used by the threat actor or shared on the dark web. There is no indication that insurance client personal information was the target of this attack. The intention of the threat actor appears to have been to obtain access to the email account in order to send further email phishing attacks to infiltrate other commercial operations, such as the unsuccessful phishing attempt against [the Organization].* 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 a third party (supply chain attack by way of compromised email account and spear-phishing). The lack of reported misuse or publication of the personal information does not mitigate against future harms as identity theft, fraud, and phishing can occur months or years after a breach.
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 identity, insurance, medical, and financial information at issue could be used to cause the harms of identity theft, fraud, and embarrassment, hurt or humiliation. Contact information, such as email addresses, could be used for the purposes of phishing or spear-phishing, increasing the affected individuals' vulnerability to the above. These are significant harms.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a third party (supply chain attack by way of compromised email account and spear-phishing). The lack of reported misuse or publication of the personal information does not mitigate against future harms as identity theft, fraud, and phishing can occur months or years after a breach.

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 all but one of the affected individuals by letter between June 10 and 18, 2021 in accordance with the Regulation. The Organization is not required to notify these individuals again.

However, the Organization reported that one affected individual could not be notified directly due to an ongoing legal matter. Instead, the Organization proposed providing indirect notice by way of delivering the notification letter to the individual's legal representative.

Section 19.1(2) of the Regulation states that "the notification may be given to the individual indirectly if the Commissioner determines that direct notification would be unreasonable in the circumstances."

Given the Organization's submission, I accept that indirect notice as described by the Organization is reasonable in this case, where the Organization is unable to contact the affected individual directly.

The Organization is required to notify the affected individual in Alberta in accordance with section 19.1(1)(b) of the *Personal Information Protection Act Regulation* and is required to confirm to my Office, within ten (10) days of the date of this decision, that the affected individual has been notified of this incident indirectly, in accordance with the requirements outlined in the Regulation.

Jill Clayton
Information and Privacy Commissioner