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	The Empire Life Insurance Company (Organization)
Decision number (file number)	P2017-ND-100 (File #001990)
Date notice received by OIPC	December 11, 2015
Date Organization last provided information	April 21, 2017
Date of decision	July 19, 2017
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)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The Organization's report of the incident identified at least the following information as being at issue: • date of birth, • medical information, and • bank information. In addition, a public notice the Organization published in the Globe and Mail stated the information at issue could include "fund values, dates of birth, addresses, medical information related to applications and claims, and social insurance numbers." Further, given the circumstances of the incident, it appears likely that customer and staff names, email addresses, and credentials are at issue. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The Organization reported that the number of affected Albertans "remains unknown. However, [the Organization] proactively assumed Albertans had been potentially affected." To the extent the information at issue was collected in Alberta, I have jurisdiction in this matter.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On November 20, 2015, several of the Organization's employees received a phishing email. • Four staff email accounts were compromised as a result of these employees opening and executing the embedded link in the phishing email. Additional phishing emails were generated and sent from the compromised staff accounts, and in at least one case, filters were set up to direct all incoming emails to trash. It does not appear that compromised email accounts were used to forward attachments or data from compromised accounts to another email address. • On December 2, 2015, an employee opened and executed the embedded link in the phishing email originally received on November 20. The compromised account was used to generate and send additional phishing emails. As a result, four additional employee accounts were compromised. • The Organization's investigation confirmed that at least one compromised employee email account contained sensitive customer personal information including date of birth, medical information and bank information.
Affected individuals	The Organization reported that the incident affected customers and financial advisors, and that the number of affected Albertans "remains unknown".
Steps taken to reduce risk of harm to individuals	• Reported incident to the Office of the Privacy Commissioner of Canada and the Canadian Anti-Fraud Centre. • Reset email account passwords to prevent further unauthorized access to accounts and enhanced authentication for email. • Blocked internal users from being able to access the phishing email and removed the phishing email from employee email accounts. • Updated security policies, launched a security education campaign on the Organization's intranet, and conducted several information security simulations. • Provided additional employee training for handling of personal information and phishing. • Enhanced IT to thwart phishing or other malicious links and attachments. • Implemented retention rules on shared "group" mailboxes to limit the amount of email in these accounts.

Steps taken to notify individuals of the incident	• Notified all employees by email sent June 17, 2016. • Published a notice in the Globe and Mail on June 17, 2016 and in La Presse on June 18, 2016. • Created a microsite with notice of the incident and provided additional information in both French and English. • Set up a call centre to receive English and French inquiries from affected customers. • Updated social media accounts with messages regarding the incident.
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 "If sensitive personal information was taken from the email accounts, it could be used for identity theft or fraud." The materials the Organization produced to notify affected individuals warn against phishing attacks and provide advice "if you ever suspect any fraudulent use of your credit card…". In my view, the identity, medical, and financial information at issue could be used to cause the harms of identity theft and fraud, as well as hurt, humiliation and embarrassment. Email addresses and credentials could be used for phishing purposes and to compromise other online accounts. 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 stated that "The individual who compromised the email accounts may have viewed or taken personal information from the email accounts. While we can confirm that the unauthorized individual did not forward emails containing personal information of individuals, we are unable to confirm whether personal information was viewed or taken from any email accounts using another method." The Organization also noted that the incident was "contained within one hour of its occurrence." In my view, the likelihood of harm resulting from this incident is increased because it was the result of malicious intent (deliberate action and installation of malware). The information may have been exposed and cannot be recovered.
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. The identity, medical, and financial information at issue could be used to cause the harms of identity theft and fraud, as well as hurt, humiliation and embarrassment. Email addresses and credentials could be used for phishing purposes and to compromise other online accounts. These are all significant harms. The likelihood of harm resulting from this incident is increased because it was the result of malicious intent (deliberate action and installation of malware). The information may have been exposed and cannot be recovered.	

The Organization is required to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified all employees by email sent June 17, 2016. In addition, the Organization provided indirect notice of the incident by:

- Publishing a notice in the Globe and Mail on June 17, 2016 and in La Presse on June 18, 2016.
- Creating a microsite with notice of the incident , and
- Updating social media accounts with messages regarding the incident.

The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner