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	Manufacturers Life Insurance Company of Canada (Organization)
Decision number (file number)	P2020-ND-005 (File #013755)
Date notice received by OIPC	October 23, 2019
Date Organization last provided information	October 23, 2019
Date of decision	February 11, 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 information at issue includes: • name, • address, • account holdings and transactions, • banking and tax slip 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	• Internal forensic investigation found evidence of anomalous activity on the Organization's Group Retirement business's Plan Member website on September 27, 2019.

	• The activity appears to be the result of common password trial and error, leveraging personal information already in the possession of the perpetrator(s). The Organization's investigation suggests a manual, "hands on" fraud effort. • The breach was discovered on October 9, 2019 when a plan member called to report unusual on line account activity.
Affected individuals	The incident affected 2 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Disabled online access to banking and tax information and the ability to process withdrawals via the website, as well as the ability to add new online contributions via the website. • Locked impacted plan members' accounts, issuing new customer identification numbers and resetting online account passwords.
Steps taken to notify individuals of the incident	Affected individuals were notified by telephone on October 10, 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 "Individuals are at risk of identity theft and potentially financial harm, however at this time our investigation suggests the perpetrator(s) came into possession of their personal information in a manner unrelated to [the Organization] or our operations. There is no evidence of successful fraudulent transactions on their [Organization] accounts." In my view, a reasonable person would consider that the financial and possibly identity information at issue could be used to cause the significant harms of identity theft and fraud.
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 the likelihood of harm resulting from this incident was "Low based on the issue as it relates to [the Organization]". In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate action). The lack of evidence of successful fraudulent transactions to date does not mitigate the potential harm from identity theft or other forms of fraud, which can occur months or even 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 financial and possibly identity information at issue could be used to cause the significant harms of identity theft and fraud.

The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate action). The lack of evidence of successful fraudulent transactions to date does not mitigate the potential harm from identity theft or other forms of fraud, which can occur months or even 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 individuals were notified by telephone on October 10, 2019. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner