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	Sun Life Assurance Company of Canada (Organization)
Decision number (file number)	P2018-ND-164 (File #010286)
Date notice received by OIPC	October 31, 2018
Date Organization last provided information	October 31, 2018
Date of decision	December 6, 2018
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. Pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA), the Organization is required to notify those individuals whose personal information was collected in Alberta.
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	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, • address, • date of birth, • member identification number, • bank account information, • account details, and • verification question and answer. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent this personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• From June 21, 2018 to August 24, 2018, the Organization discovered 36 fraudulent attempts made by individuals who called the Customer Service Centre to obtain login information and/or withdraw funds from client accounts. These individuals impersonated actual clients when attempting to obtain access to a client account for financial gain. • The Organization stopped all attempts to withdraw funds except for one which resulted in a fraudulent withdrawal.
Affected individuals	The incident affected 36 individuals across Canada, including one (1) in Alberta.
Steps taken to reduce risk of harm to individuals	• Suspended online and mobile access to the clients' accounts until the accounts could be re-secured. • Offered prepaid 24 months subscriptions to credit monitoring service. • Engaged the bank involved and reported the matter to police. • Continued monitoring of the activity and transactions on the affected clients' accounts.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter mailed the week of October 29, 2018.
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 potential harms could include "Identity fraud and financial loss". In my view, a reasonable person would consider that the contact, identity, financial and credential information could be used to cause the significant harms of identity theft and fraud. Compromised verification question and answer could make other accounts, including online accounts, vulnerable.
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.	In its report, the Organization noted that "A single fraudulent withdrawal was processed under one impacted client's …account'. Further, "Identifying information that the imposters had in their possession prior to contacting [the Organization] could be used to attempt fraudulent transactions or identity fraud involving other financial institutions." In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because the incident resulted from malicious intent (deliberate action by an unauthorized party) and, in one case at least, resulted in a fraudulent withdrawal.

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, financial and credential information could be used to cause the significant harms of identity theft and fraud. Compromised verification question and answer could make other accounts, including online accounts, vulnerable. The likelihood of harm resulting from this incident is increased because the incident resulted from malicious intent (deliberate action by an unauthorized party) and, in one case at least, resulted in a fraudulent withdrawal. I require the Organization to notify the affected individuals whose information was collected in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand affected individuals were notified by letter mailed the week of October 29, 2018. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner