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)	P2015-ND-35 (Case File #P2772)
Date notice received by OIPC	July 15, 2014
Date Organization last provided information	July 15, 2014
Date of decision	May 19, 2015
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 pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The organization is federally incorporated and licenced under the *Alberta Insurance Act* to carry on business in Alberta. I have jurisdiction because the Organization is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • address, • date of birth, • Social Insurance Number (SIN), • insurance policy number and value. This information is "personal information" as defined in section 1(1)(k) of PIPA and was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• The Organization reported that a corporate laptop, containing the personal information at issue, was stolen on June 23, 2014 from an employee's car. • The laptop was password protected and encrypted. • The encryption key and the previous password were written down and stored with the laptop at the time of the theft. The previous password was a single digit different from the one protecting the laptop, making the new one easy to predict.
Affected individuals	A total of 810 individuals were affected by the incident; 5 of the affected individuals are residents of Alberta.
Steps taken to reduce risk of harm to individuals	• The laptop was password protected and encrypted. • The password was reset the next day. • The computer was configured to lock a user's account after five failed login attempts. Only an authorized IT support staff with the right level of permission could unlock the account. • The incident was reported to law enforcement authorities. • Affected individuals were advised to review their credit records and report suspicious activities. • A free credit report and a one-year credit monitoring subscription with TransUnion were provided to affected individuals.
Steps taken to notify individuals of the incident	Written notifications were mailed to affected individuals in the week of July, 14 2014.
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 affected individuals were at risk of identity theft or fraud. In my view, the personal information involved is sensitive. It contains identity (SIN) and insurance information. The types of harm that could result from this incident include identity theft, fraud and/or hurt and humiliation. In my view, 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	The Organization reported that due to the sensitivity of the information involved there is a real risk of significant harm to affected individuals. In my view, the likelihood of harm resulting from this incident is increased because the laptop was stolen. Further, although the laptop was encrypted, the previous password and encryption

incident and the possible harm.	key were written down and stored with the laptop at the time of the theft. The previous password was a digit different from the one protecting the laptop. The personal information stored on the device was, therefore, vulnerable to unauthorized access.

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 personal information involved sensitive identity (SIN) and insurance information that could be used to cause the significant harms of identity theft, fraud and/or hurt and humiliation. The incident resulted from malicious intent (i.e. the laptop was stolen). Further, although the laptop was encrypted, the previous password and encryption key were written down and stored with the laptop at the time of the theft. The previous password was a digit different from the one protecting the laptop. The personal information stored on the device was, therefore, vulnerable to unauthorized access. These factors contributed significantly to my decision.

I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified the individuals who were affected, in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner