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)	P2016-ND-25 (File #000268)
Date notice received by OIPC	February 12, 2015
Date Organization last provided information	February 17, 2015
Date of decision	March 16, 2016
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 out business in Alberta. 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, • policy number and value, • Social Insurance Number (SIN). This information is about identifiable individuals and qualifies as "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• An employee of the Organization was a victim of a social engineering attack on January 1, 2015. • The employee received a message about a potential virus on the Organization-issued laptop she was using. The message advised her to call her internet service provider (ISP) using a number that was part of the message. • She called the number and spoke to an individual who, posing as the employee's ISP, advised her to purchase anti-virus and anti-hacking software. • She purchased the software using her credit card and provided remote access to her computer to the individual for about two hours to install the software and run virus scans. • Three weeks later, the purchased products expired and she reported the incident to her employer on January 21, 2015. • The Organization determined that she was a victim of a social engineering attack as the authenticity of the ISP could not be established. • The individual posing as the ISP and the software installed on the laptop could have accessed personal information stored on the device (laptop). • The Organization reported that it did not find evidence of unauthorized access on the laptop but cannot ascertain that personal information was not accessed.
Affected individuals	Twenty-eight (28) individuals in Alberta were affected.
Steps taken to reduce risk of harm to individuals	• The Organization recalled the laptop and conducted an investigation. • It was determined that the laptop was not connected to the Organization's network when it was remotely accessed by the unauthorized individual. • The laptop was re-imaged on January 22, 2015 to remove the potentially malicious program that had been installed. • The laptop was encrypted.
Steps taken to notify individuals of the incident	Notification letters were sent to affected individuals.
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	The Organization reported that the "potential harm may include: financial loss, fraud and identity theft" and "the potential harm that could result from the breach is significant due to the circumstances." I agree with the Organization's assessment. The personal

must be important, meaningful, and with non-trivial consequences or effects.	information at issue includes sensitive identity information that could be used to cause the harms of identity theft, fraud and financial loss. 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.	In assessing the likelihood that harm could result from this incident, the Organization reported that it has no means to confirm whether the intruder accessed data on the laptop; however, there was unauthorized access for approximately 2 hours. In my view, the likelihood of harm resulting from this incident is increased because the laptop was accessed by an unauthorized individual with malicious intent, who also installed software on the computer that was not approved by the Organization. If the software was malicious, it may have transferred personal information from the computer (and potentially the Organization's network if the compromised computer was connected to the network before it was re-imaged) to a remote location. The Organization cannot confirm that personal information stored on the laptop was not accessed by the unauthorized individual, and information stored on the laptop was exposed for 2 hours.

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 at issue includes sensitive identity information that could be used to cause the significant harms of identity theft, fraud and financial loss. The likelihood of harm is increased because the laptop was accessed by an unauthorized individual with malicious intent who also installed software. The Organization cannot confirm that personal information stored on the laptop was not accessed by the unauthorized individual, and information stored on the laptop was exposed for 2 hours.

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 affected individuals in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner