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-151 (File #009842)
Date notice received by OIPC	September 25, 2018
Date Organization last provided information	September 25, 2018
Date of decision	November 23, 2018
Summary of decision	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify the individual pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
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. The incident occurred in Alberta.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • first and last name, • date of birth, • policy reference number, and • telephone number. This information is about an identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• On June 26, 2018, an employee of the Organization emailed a beneficiary designation form to a client. • The form was pre-filled with the first and last name of the recipient, and the date of birth, telephone number and two policy reference numbers belonging to another client who shares the same first and last name.

	• The incident was discovered on July 11, 2018 when the unauthorized recipient emailed his advisor to report the error.
Affected individuals	The incident affected one individual.
Steps taken to reduce risk of harm to individuals	• Wrote to the unauthorized recipient requesting that he delete the email attachment at issue and confirm when the action was taken (an attestation form was also provided). To date, the Organization has not received a response. • Reviewed the handling of the original request with the employee, and the impact of the incident on the recipient and the impacted client. Provided coaching specific to the error that caused the incident. The employee also completed online privacy and cyber security training. • A refresher training course will be rolled out during the fourth quarter of 2018. • Offered credit monitoring services to the affected individual.
Steps taken to notify individuals of the incident	The affected individual was notified by telephone on July 16, 2018 and by letter dated July 27, 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 identified the type of harm that may result from the incident as "identity theft or financial fraud". I agree with the Organization's assessment. The identity and insurance 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 did not specifically assess the likelihood of harm resulting from this incident. In my view, a reasonable person would consider that the likelihood of harm is decreased as the incident did not result from malicious intent, but rather human error, and the unauthorized recipient reported the error to the Organization. However, the Organization has not been able to confirm the information was securely destroyed.
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 in this case.	

The identity and insurance information at issue could be used to cause the significant harms of identity theft and fraud. A reasonable person would consider that the likelihood of harm is decreased as the incident did not result from malicious intent, but rather human error, and the unauthorized recipient reported the error to the Organization. However, the Organization has not been able to confirm the information was securely destroyed.

I require the Organization to notify the affected individual in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the affected individual was notified by telephone on July 16, 2018 and by letter dated July 27, 2018. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner