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 Financial (Organization)
Decision number (file number)	P2018-ND-086 (File #004903)
Date notice received by OIPC	January 27, 2017
Date Organization last provided information	February 28, 2017
Date of decision	July 18, 2018
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 pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is incorporated in Alberta and is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • address, • plan identification number, • payroll number, • date of birth, • hire date, • salary, • coverage amounts of life and disability insurance, • premiums, and • beneficiary and dependent information. This information is about identifiable individuals and is "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	• On November 15, 2016, an employee of the Organization inadvertently sent a client a pdf file containing his own coverage summary along with those for 28 other clients. • A second client was inadvertently emailed a pdf file containing his own coverage summary along with those for 56 other clients. • The first recipient reported the error to his Plan Sponsor on January 11, 2017. The Plan Sponsor informed the Organization on the same date. • The second recipient terminated employment with the Plan Sponsor on November 30, 2016 and did not inform the Plan Sponsor of the incident before his departure. However, the Plan Sponsor was able to confirm the second unauthorized recipient deleted the email prior to leaving his employment and that the email was not forwarded. • The Organization received confirmation from the two unintended recipients on January 27, 2017 and January 30, 2017 respectively, that they deleted and did not forward or make a copy of the information at issue.
Affected individuals	The incident affected 57 individuals, of which 31 are residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Contacted the unintended recipients by mail and telephone. • Confirmed the containment of the breach. • Placed a note on the affected clients' files so that any inquiry made on the client file is subject to deeper verification. • Notified affected individuals of the incident and offered a 12 month subscription for a credit monitoring service. • Notified the Plan Sponsor and other privacy commissioners.
Steps taken to notify individuals of the incident	The affected individuals were notified on January 25, 2017 by email and by regular mail.
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 "The risk that the information was shared with a colleague known to the recipient may cause hurt, humiliation and negatively impact the affected individual's reputation." I accept the Organization's assessment. The contact and employment information at issue could be used to cause the harms of hurt, humiliation and embarrassment. Identity information could be used to cause the harms of identity theft and fraud. These are all 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.	The Organization reported its assessment that "At this time (the Organization) has no evidence of misuse if the information by the recipients. However, having discovered the incident 8 weeks after it occurred, and the efforts to contain the breach are in progress, the harm that could result is hurt, humiliation and damage to the impacted individual's reputation. The risk of harm of identity theft and fraud is low given the nature of the information and the individuals involved." I agree that the likelihood of identity theft and fraud in this case is low, given that the incident did not result from malicious intent but rather human error, and the Organization was able to confirm with both unintended recipients that the information was deleted, and neither forwarded nor copied. However, the likelihood of hurt, humiliation and embarrassment is high given that the affected individuals and the unintended recipients are likely to have professional/and personal relationships.

DECISION UNDER SECTION 37.1(1) OF PIPA

Given the information reported by the Organization I have concluded that there is a real risk of harm in this case.

The contact and employment information at issue could be used to cause the harms of hurt, humiliation and embarrassment. Identity information could be used to cause the harms of identity theft and fraud. These are all significant harms. The likelihood of identity theft and fraud in this case is low, given that the incident did not result from malicious intent but rather human error, and the Organization was able to confirm with both unintended recipients that the information was deleted, and neither forwarded nor copied. However, the likelihood of hurt, humiliation and embarrassment is high given that the affected individuals and the unintended recipients are likely to have professional/and personal relationships.

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

I understand affected individuals were notified on January 25, 2017 by email and by regular mail. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner