



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Sun Life Global Investments (Organization)
Decision number (file number)	P2017-ND-145 (File #006666)
Date notice received by OIPC	September 25, 2017
Date Organization last provided information	September 25, 2017
Date of decision	November 6, 2017
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 <i>Personal Information Protection Act</i> (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA “organization”	The Organization is an “organization” as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA “personal information”	<p>The incident involved all or some of the following information:</p> <ul style="list-style-type: none">• name,• address,• account number(s),• account value, and• transaction history. <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA. Some of the information was collected in Alberta.</p>
DESCRIPTION OF INCIDENT	
<input type="checkbox"/> loss <input type="checkbox"/> unauthorized access <input checked="" type="checkbox"/> unauthorized disclosure	
Description of incident	<ul style="list-style-type: none">• Between August 14, 2017 and August 19, 2017, the Organization mailed a number of client statements to the wrong clients.• The incident was reported to the Organization on August 18, 2017 by a client who received his own statement, along with that of another client.

	<ul style="list-style-type: none"> The Organization investigated and found the error resulted from a data mis-match during the third-party vendor statement production process.
Affected individuals	The incident affected seventy-six (76) clients, including 11 residents of Alberta.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> Wrote to the unintended recipients who received statements in error and requested confirmation that they securely destroyed the statements and that the contents had not been used or shared. Offered free, 1-year credit monitoring service subscriptions to affected individuals. The vendor identified the cause of the incident and implemented the necessary process to prevent the situation from reoccurring. The Organization will oversee the testing of the process change and ensure quality control requirements are followed.
Steps taken to notify individuals of the incident	The Organization notified affected individuals by letter on September 13, 2017.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
<p>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.</p>	<p>The Organization reported that the information at issue “... could be used to attempt financial fraud”.</p> <p>I accept the Organization’s assessment that the information at issue could be used to cause financial fraud. This is a significant harm.</p>
<p>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.</p>	<p>The Organization reported that “To date, no fraud has been reported or identified...”.</p> <p>In my view, although the incident resulted from an unintentional mailing error and not malicious intent, the likelihood of harm is increased considering the number of unintended recipients (70), and because the Organization did not report receiving confirmation from most, if not all, unintended recipients that the information was not used or shared, and was securely destroyed.</p>
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 information at issue could be used to cause the significant harm of financial fraud. Although the incident resulted from an unintentional mailing error and not malicious intent, the likelihood of harm is increased considering the number of unintended recipients (70), and because the Organization did not report receiving confirmation from most, if not all, unintended recipients that the information was not used or shared, and was securely destroyed.

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 the affected individuals were notified by letter on September 13, 2017. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner