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	AZGA Service Canada Inc., operating as Allianz Global Assistance (Organization). The Organization is a service provider to Manulife Financial. The latter confirmed the Organization had "control" of the information at issue and the responsibility to report the incident under section 34.1 of the *Personal Information Protection Act* (PIPA).
Decision number (file number)	P2015-ND-15 (File #P2354)
Date notice received by OIPC	May 2, 2013
Date Organization last provided information	December 12, 2013
Date of decision	November 10, 2015
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 PIPA.
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is registered in Alberta and qualifies as an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	This incident involved the following information: • name, • address, • group plan number, • individual's certificate number (this is the same as the individual's social insurance number, or SIN). This information is about an identifiable individual and qualifies as "personal information" as defined in section 1(1)(k) of PIPA.

DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	On May 2, 2013 the Organization inadvertently mailed Explanation of Benefit forms, containing the personal information at issue, to the wrong individuals. The error resulted from an incorrect setting on the Organization's mailing machine which caused unrelated documents to be placed in one envelope. The error was discovered on May 7, 2013.
Affected individuals	A total of 381 individuals throughout Canada were affected by this incident, including one (1) resident of Alberta.
Steps taken to reduce risk of harm to individuals	• Manual controls for sending letters were enhanced to include recording all outgoing mail counts together with staff sign-off. The mailroom manager reviews, verifies and signs as evidence that manual controls have been completed. On a weekly basis, completed forms are submitted to the Compliance department for independent verification. • Additional training of mail staff was conducted to insure proper mailing procedures. • The affected individual was offered one year free credit monitoring.
Steps taken to notify individuals of the incident	The Organization notified the affected individual by letter on May 31, 2013.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the 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 the type of harm that could result from breach is identity theft. I agree with the Organization. The personal information includes sensitive identity information which could be used to cause the harms of identity theft and fraud. 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.	The Organization reported the likelihood of harm resulting from this incident is low and noted the individual's certificate number was not identified as a social insurance number in the document. In my view, there is a real risk of harm resulting from this incident. Although the incident was the result of human error and not malicious intent, the risk of harm is increased because the Organization was not able to identify who received the information in error, and therefore could not confirm the information was destroyed and not disclosed further. The information was not recovered.

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 resulting from this incident. The personal information could be used to cause the significant harms of identity theft and fraud. Although the incident was the result of human error and not malicious intent, the risk of harm is increased because the Organization was not able to identify who received the information in error, and therefore could not confirm the information was destroyed and not disclosed further. The information was not recovered.

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 Organization notified the affected individual on June 11, 2013 in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner