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	The Presbyterian Church in Canada (Organization)
Decision number (file number)	P2018-ND-133 (File #009889)
Date notice received by OIPC	September 26, 2018
Date Organization last provided information	September 26, 2018
Date of decision	October 16, 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 an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information about two residents of Alberta: • name, • Social Insurance Number, • member status, • member status date, • hire date, • service date, • plan entry date, • normal retirement date, • employer, • province of employment, • job category, and • job position. 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	• The Organization contracts with a third party, Eckler Ltd., to develop and host its pension administration system. • On June 13, 2018, Eckler advised the Organization that an internal audit of its privacy practices revealed that it had inadvertently disclosed the personal information of certain of the Organization's members in two separate incidents. • The first incident occurred on November 18, 2011 when six (6) copies of a response to a client request for proposal were sent out that contained screenshots of the Organization's pension system's user guide. Although it was not known at the time, the guide contained actual personal information of the Organization's pension members instead of fictitious dummy data. • The second incident occurred on May 30, 2012 when Eckler sent a prospective client an email containing the guide. This version of the guide also contained the personal information of the Organization's pension members. This email was sent to two (2) individuals at the prospective client organization and was marked 'confidential'. • The breach was discovered on June 6, 2018 when Eckler performed an audit of user guides. Eckler reported the breach to the Organization on June 13, 2018.
Affected individuals	The incident affected 7 individuals, including 2 who were residents of Alberta at the time of the incident.
Steps taken to reduce risk of harm to individuals	• Sought further information from Eckler and asked them to investigate the breaches, and engaged with Eckler to confirm the personal information at issue, contain the breach and mitigate risk. • Engaged separate privacy counsel. • Eckler has agreed to contact clients that received the guide to request that they destroy or delete copies that might still be in their possession. Eckler will also follow up to confirm that clients have taken such steps. • Eckler reaffirmed its commitment to protecting the confidentiality of all personal information in its possession, and its policy to never use personal information in its system user guides. • No client-branded user guides will be used by Eckler as samples in future proposal submissions without the express, written permission of the client.

	• Eckler has assured the Organization that a 'sanitized' sample user guide has been drafted for use in future proposals. Individuals who prepare this type of documentation have also been provided additional training from Eckler regarding required privacy practices • At the Organization's request, Eckler agreed to provide the affected individuals with credit monitoring services.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter sent September 26, 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 reported that "Due to the loss of social insurance number, there is potential harm of identity theft and fraud." I agree with the Organization's assessment. The identity (social insurance number) and employment 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 reported that "While the breaches were discovered in June 2018, they occurred in 2011 and 2012. The [Organization] is not aware of any subsequent harm to the individuals involved. As exposure was limited, it is our assessment that the likelihood of signifcant [sic] harm is very low at this time." The Organization also reported that "Eckler advised us that the original RFP included a non-disclosure clause that required the potential client to hold in confidence all information submitted by bidders (including Eckler) in its response to the tender." In my view, the likelihood of significant harm resulting in this case is increased despite the fact the breach was not the result of malicious intent, and the RFP included a non-disclosure clause. The information at issue has potentially been exposed for seven and six and a half years respectively and may have been further disclosed to unknown parties. Had the Organization been made aware of the breach earlier, steps could have been taken to immediately contain the breach and to recover or ensure the secure destruction of the information provided to unauthorized recipients.

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 identity (social insurance number) and employment information at issue could be used to cause the significant harms of identity theft and fraud. The likelihood of significant harm resulting in this case is increased despite the fact the breach was not the result of malicious intent, and the RFP included a non-disclosure clause. The information at issue has potentially been exposed for seven and six and a half years respectively, and may have been further disclosed to unknown parties. Had the Organization been made aware of the breach earlier, steps could have been taken to immediately contain the breach and to recover or ensure the secure destruction of the information provided to unauthorized recipients. The Organization is required to notify the affected individuals whose persona information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand affected individuals were notified by letter sent September 26, 2018. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner