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	Combined Insurance Company of America (Organization)
Decision number (file number)	P2020-ND-049 (File #013681)
Date notice received by OIPC	October 31, 2019
Date Organization last provided information	December 13, 2019
Date of decision	May 21, 2020
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those individuals whose personal information was collected in Alberta, 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 all or some of the following information: • name, • age, • occupation, • number of dependents and ages, • existing insurance coverage including amounts and insurer names, • income, asset and liability amounts, • calculation of life insurance needs and recommendations. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	

Description of incident	• The Organization takes electronic insurance policy applications from consumers in the normal course of business. Typically, an agent will meet with a consumer to complete an application, including a needs analysis. Information is uploaded to the Organization's e-Agent platform. • In September 2019, as part of a routine compliance audit, staff noticed 3 instances where the name on the needs analysis document did not match the name on other policy documents. Further investigation found that if an agent failed to properly clear the needs analysis information for a previous customer, the previous customer's information might inadvertently become associated with a new applicant. • The breach occurred between November 2017 and September 2019. The problem was identified September 18, 2019. • The Organization reported it was not aware of any actual or attempted misuse of the personal information at issue.
Affected individuals	The Organization identified 642 instances where the problem may have occurred, and reported the incident affected 75 individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Issued a bulletin to ensure sales representatives are aware of the proper process. • Flagged all customer files associated with the incident. • Implemented a temporary fix to manually review documents and planned for a permanent fix in October 2019. • Provided affected individuals with information to protect against identity theft. • Offered one free year of credit monitoring and identity protection services. • Reported the incident to provincial and federal Privacy Commissioners.
Steps taken to notify individuals of the incident	Affected individuals were notified verbally or in writing on December 13, 2019 with mailings to be staggered over the weeks.
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: *Summary insurance coverage information and agent assessments of required coverage would not normally be considered to be particularly sensitive. While the existing insurance coverage and unverified financial data may be considered to be sensitive to the applicant, the nature of the data and the circumstances of the disclosure would not appear to give rise to any real risk of significant harm…In this regard, the data does not contain the type of key identifiers that can typically be exploited by identity thieves…and it is unlikely that the form would provide*

	enough information for a recipient to be able to identify the individual to which the needs assessment relates using other available information (unless the individual has an unusual name or a narrow occupational category, etc.). In my view, a reasonable person would consider that the contact information, as well as information about existing insurance coverage and reported income, assets and liabilities is comprehensive enough that it could be used to cause the significant harms of identity theft and fraud, as well as potentially hurt, humiliation and embarrassment.
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 forms were disclosed only to a limited number of other applicants for insurance (in most cases just to one applicant), and based on the length of time the issue has apparently existed, the number of packages that appear to have been mailed out to mismatched needs analysis forms, the lack of complaints or inquiries, and the limited utility of the needs assessment after the policy has been issued, it appears in many cases applicants may not even be aware that they received a needs assessment for another person.* In my view, there is a real risk of significant harm in this case, despite the fact the incident did not result from malicious intent. It is not clear, however, whether the Organization retrieved the information that was disclosed in error or confirmed the information was destroyed and not used or distributed further. The information may have been exposed for approximately twenty (20) months. The lack of reported incidents to date does not mitigate against future harmful use of the information.

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.

A reasonable person would consider that the contact information, as well as information about existing insurance coverage and reported income, assets and liabilities is comprehensive enough that it could be used to cause the significant harms of identity theft and fraud, as well as potentially hurt, humiliation and embarrassment. Although the likelihood of harm is decreased as the incident did not result from malicious intent, it is not clear whether the Organization retrieved the information that was disclosed in error or confirmed the information was destroyed and not used or distributed further. The information may have been exposed for approximately twenty (20) months. The lack of reported incidents to date does not mitigate against future harmful use of the information.

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

I understand the Organization notified affected individuals verbally and in writing starting December 13, 2019, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner