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)	P2021-ND-197 (File #018193)
Date notice received by OIPC	November 19, 2020
Date Organization last provided information	November 19, 2020
Date of decision	October 15, 2021
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify 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 the following information: • name, • agent code and position, • home address, • business telephone number, • partial birth date (month & day only), • email address, • spouse's name (if applicable), • highest internal award earned, • department, and • manager's name. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. Some of the information appears to qualify as "business contact information" as defined in section 1(1)(a) of PIPA to mean "an individual's name, position name or title, business telephone number, business address, business e mail address, business fax number and other similar business information."

	Section 4(1)(d) of PIPA says that the Act does not apply to the collection, use and disclosure of business contact information "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." In this case, I considered that the possible unauthorized access to the information was not "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." As a result, PIPA applies.
DESCRIPTION OF INCIDENT	
☐ loss ☐ unauthorized access ☒ unauthorized disclosure	
Description of incident	• On Friday, October 30, 2020, an employee sent an email and mistakenly added the contact list of email recipients to the email itself. • The list contained contact information of 415 individuals (independent contractors) and was emailed to all 415 individuals on the list. The contact list was not password protected. • The employee who sent the email discovered the error and tried to recall it. • On November 2, 2020, an email was sent to all recipients of the email instructing each of them to delete the original email and its attachment, to not retain any of the information contained in the email in any form, and to not disclose said information to any third party. Recipients were also asked to confirm deletion of the original email and its attachments without retaining or disclosing any of its contents. • All responses are currently being tracked and followed up on.
Affected individuals	The incident affected 415 individuals, including 271 individuals whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Attempted to recall the email. • Sent a follow up email requesting confirmation that the recipients deleted and did not circulate the information. • Recommended that contact lists be password protected going forward. In addition, passwords should be applied to other spreadsheets and documents containing personal information. • Provided information to affected individuals on how to request credit reports and protect themselves against identity theft and fraud.

Steps taken to notify individuals of the incident	The affected individuals were notified by mail beginning on November 12, 2020.
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 "The combination of personal emails, contact information, spouse's and manager's name increases the risk of the information being used for phishing or fraud." I accept the Organization's assessment that a reasonable person would consider that the contact information, including email address, and particularly in conjunction with employment information, could be used to send unsolicited emails and for phishing purposes, leading to an increased risk of identity theft and fraud. Contact information, along with awards earned could be used to cause reputational harm and embarrassment. 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: *Since all the independent contractors on the list received the information, which includes their own information, and we will be tracking all responses, the risk of misuse is low, but not impossible.* In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is decreased as the breach resulted from human error and not malicious intent. The Organization requested that each unintended recipient delete the original email and its attachment, not retain any of the information contained in the email in any form, and not disclose said information to any third party. The email also requested each recipient confirm deletion of the original email and its attachments without retaining or disclosing any of its contents. It is unclear whether all the unintended recipients followed the Organization's instructions. The fact the unintended recipients are independent contractors of the Organization reduces the likelihood of phishing. The likelihood of reputational harm and embarrassment to the affected individual is increased, however, given the unintended recipients and affected individuals are all independent contractors of the same Organization.
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, including email address, and particularly in conjunction with employment information, could be used to send unsolicited emails	

and for phishing purposes, leading to an increased risk of identity theft and fraud. Contact information, along with awards earned could be used to cause reputational harm and embarrassment. These are all significant harms.

The likelihood of harm resulting from this incident is decreased as the breach resulted from human error and not malicious intent. The Organization requested that each unintended recipient delete the original email and its attachment, not retain any of the information contained in the email in any form, and not disclose said information to any third party. The email also requested each recipient confirm deletion of the original email and its attachments without retaining or disclosing any of its contents. It is unclear whether all the unintended recipients followed the Organization's instructions. The fact the unintended recipients are independent contractors of the Organization reduces the likelihood of phishing. The likelihood of reputational harm and embarrassment to the affected individual is increased, however, given the unintended recipients and affected individuals are all independent contractors of the same Organization.

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 affected individuals were notified by mail beginning on November 12, 2020. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner