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	TAWS Security (Organization)
Decision number (file number)	P2018-ND-088 (File #009226)
Date notice received by OIPC	July 18, 2018
Date Organization last provided information	July 18, 2018
Date of decision	July 26, 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 operates in Alberta and 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, • address, • employee earnings, • date of birth, • beneficiary, and • spouse. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• On July 18, 2018, an employee of the Organization sent an email to 17 employees asking them to complete attached benefit forms. Inadvertently, the forms that were attached contained completed documents with the information at issue for 14 other individuals.

	• The employee quickly realized the error and tried to retract the email but was unsuccessful. The unauthorized recipients were told to disregard the email.
Affected individuals	The incident affected 14 individuals.
Steps taken to reduce risk of harm to individuals	• Attempted to retract the email. Asked unauthorized recipients to disregard the email and reminded them of signed confidentiality agreements. They will also be requested to send an email confirming the deletion of the confidential information. • Informed the COO, employment standards, and the Information and Privacy Commissioner. • Enabling "read receipt" and "undo send" on email account. Double checking all attachments.
Steps taken to notify individuals of the incident	Affected individuals were notified by email sent July 18, 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 "Employees affected may feel violated, other employees will now know personal information. Employees may feel untrustworthy of the person responsible for this breach". Further, "The sensitive information cannot result in identity theft because SIN numbers are not included. Credit Cards were not contained in the information that was emailed." In my view, the identity (date of birth) information, in conjunction with other information, could be used to cause the harms of identity theft and fraud. The employment information (earnings) could be used to cause the harms of hurt, humiliation 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.	In assessing the likelihood of harm resulting, the Organization noted a number of factors, including that "There was no malicious intent on the email that was accidently sent out", "The information was not recovered" and " 'undo send' email was not enabled, and if it was, it would have to be caught within 30 seconds of the email being sent." In my view, the likelihood of identity theft and fraud in this case is low, given that the incident did not result from malicious intent but rather human error, and the Organization knows the unauthorized recipients. However, the likelihood of hurt, humiliation and embarrassment is high given that the affected individuals and the unintended recipients are likely to have professional/and personal relationships.

DECISION UNDER SECTION 37.1(1) OF PIPA
Given the information reported by the Organization I have concluded that there is a real risk of significant harm in this case. The identity (date of birth) information, in conjunction with other information, could be used to cause the harms of identity theft and fraud. The employment information (earnings) could be used to cause the harms of hurt, humiliation and embarrassment. These are all significant harms. The likelihood of identity theft and fraud in this case is low, however, given that the incident did not result from malicious intent but rather human error, and the Organization knows the unauthorized recipients. However, the likelihood of hurt, humiliation and embarrassment is high given that the affected individuals and the unintended recipients are likely to have professional/and personal relationships. 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 affected individuals were notified by email sent July 18, 2018. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner