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	1883865 Alberta Ltd. / Knoxville's Tavern (Organization)
Decision number (file number)	P2020-ND-169 (File #016797)
Date notice received by OIPC	March 9, 2020
Date Organization last provided information	March 9, 2020
Date of decision	December 1, 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, • address, • Social Insurance Number, and • income. 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 February 28, 2020, due to a technical error, the Organization emailed employee T4s to incorrect recipients (past and / or present employees).

	• The incident was discovered the same day when an employee reported receiving the wrong person's T4. • At the time of the report, the Organization did not confirm whether all recipients of the erroneously delivered T4s permanently deleted the record, as requested in the Organization's notification emails.
Affected individuals	The incident affected 260 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Sent multiple notification emails, including advice to delete the erroneously delivered records. • Offered credit and identity monitoring services to each affected employee. • Implemented redundancy protocols to ensure file formats are consistent, and align with correct employee identifiers, prior to integration of data.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on February 28, March 3, and March 6, 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 "A recipient of someone else's data could distribute their PI publicly and/or use SIN # to establish credit and/or other fraudulent purposes." I agree with the Organization's assessment. A reasonable person would consider the identity and financial information at issue could be used for the purposes of identity theft, fraud, as well as hurt, humiliation and embarrassment. 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: "As each persons [sic] PI was shared with ONLY ONE person, we feel the risk is very low, and that fellow employees will delete the records (T4) received as requested. We do know WHO received WHOSE PI, and can therefore initiate action directly against someone should they release the person's PI that they received in error." 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, but rather, human error (data integration error). The Organization did not confirm whether all T4s delivered in error were deleted and there may be personal or professional relationships between affected individuals and unintended recipients, increasing the likelihood of hurt, humiliation, or embarrassment.

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 the identity and financial information at issue could be used for the purposes of identity theft, fraud, as well as hurt, humiliation and embarrassment. These are significant harms. There is a real risk of significant harm in this case, despite the fact the incident did not result from malicious intent, but rather, human error (data integration error). The Organization did not confirm whether all T4s delivered in error were deleted and there may be personal or professional relationships between affected individuals and unintended recipients, increasing the likelihood of hurt, humiliation, or embarrassment. 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 in a series of emails dated February 28, March 3, and March 6, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner