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	Aramark Entertainment Services (Canada) Inc., a subsidiary of Aramark Canada Ltd. (Organization)
Decision number (file number)	P2018-ND-038 (File #003887)
Date notice received by OIPC	September 8, 2016
Date Organization last provided information	September 8, 2016
Date of decision	March 2, 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 those 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 all or some of the following information: • name, • home address, • telephone number, • email address, • date of birth, • job title, • social insurance number (SIN), and • banking information. 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 August 19, 2016, an employee with the Organization sent an email to forty-nine (49) new employees regarding an upcoming training session.

	• On August 26, 2016, the Organization received a report that a zip file attached to the email contained the personal information of sixty-four (64) other employees of the Organization. • The employee who sent the email was unaware of the contents of the attachment. • The personal information in the file was not properly secured or protected by restricted access. • On August 31, 2016, the Organization emailed the recipients of the email and instructed them to disregard the file and to delete and/or destroy any electronic or hard copies they may have had of the file.
Affected individuals	The incident affected 64 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Sent an email to the recipients instructing them to disregard, delete and/or destroy the file. • Secured the file and restricted access to a limited number of employees. • Providing privacy training with an emphasis on best practices for managing and storing employee personal information.
Steps taken to notify individuals of the incident	Affected individuals were notified by email (if email was provided) followed by a hard copy of the breach notification via courier, on September 7, 2016.
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 possible harm that might result from this incident include "identity theft, fraud, financial loss and negative effects on their credit record." I agree with the Organization. The contact, identity and banking information could be used to cause identity theft, fraud, financial loss and negative effects on credit reports. Further, email addresses could be used for phishing purposes. 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 that "We do not believe the likelihood of harm is high. The recipients of the personal information are 49 other …employees - so it was a limited recipient list. As the information breach occurred due to the inadvertence of an … employee there is no risk of an ongoing breach, nor was there any malicious intent behind the breach." The Organization also stated that "should harm occur, it could be significant based on the type of information involved."

	I agree with the Organization that the likelihood of harm resulting from this incident is reduced because the incident resulted from human error, rather than malicious intent. However, the Organization did not confirm with all recipients that the information was not accessed, copied, used or shared, and that it was in fact deleted or destroyed.

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 contact, identity and banking information could be used to cause identity theft, fraud, financial loss and negative effects on credit reports. Further, email addresses could be used for phishing purposes. These are all significant harms. The likelihood of harm resulting from this incident is reduced because the incident resulted from human error, rather than malicious intent. However, the Organization did not confirm with all recipients that the information was not accessed, copied, used or shared, and that it was in fact deleted or destroyed.

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 the Organization notified affected individuals in an email and/or letter dated September 7, 2016 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner