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	Keyera Corp. (Organization)
Decision number (file number)	P2021-ND-275 (File #018579)
Date notice received by OIPC	December 7, 2020
Date Organization last provided information	December 7, 2020
Date of decision	February 16, 2022
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 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 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 some or all of the following information: <u>Employees:</u> • first and last name, • home address, • date of birth, • gender, • marital status, • salary information, • insurance information, and • dependents. <u>Dependents:</u> • first and last name, • date, of birth, • gender, and • relationship to employee. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent this information was collected in Alberta, PIPA applies.

DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• On October 27, 2020, the Organization's human resources team uploaded certain personal employee information via a secure portal to a new group benefits and insurance provider for migration into the service provider's systems. • On November 4, 2020, an employee of the service provider inadvertently emailed a document containing the information at issue to an incorrect email address. • The service provider confirmed the email was received by an active account in the "Hotmail" domain. • The service provider advised the Organization of the breach on November 30, 2020.
Affected individuals	The incident affected 2,690 individuals.
Steps taken to reduce risk of harm to individuals	The Organization reported it will provide anti-phishing training for employees, as necessary. The service provider: • tried to recall the email and to confirm destruction. • committed to offering 5 years of credit monitoring services to the Organization's affected employees and their dependents. • is adding authentication measures to the Organization's insurance portal. • will review its information transfer protocol with employees, and will include a reminder that sensitive information should be transmitted via shared drives as opposed to email unless proper encryption is used. • is implementing a Data Loss Prevention solution, so that emails containing personal information will be blocked from leaving the network.
Steps taken to notify individuals of the incident	The affected employees were notified by email on December 7, 2020. The Organization also reported, "As the Organization does not have contact information for each employee's dependents, the notice included the Organization's request that employees relay the information and risk mitigation strategies described in the notice to his or her dependents, as necessary."

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, *Release of each employee's first and last name, home address, and salary information could result in humiliation and/or reputational harm.* *Release of each employee's first and last name, home address, gender, birthdate and insurance information could result in identity theft and/or fraud.* *Release of each employee's full name and home address could result in physical harm to the employee.* *Release of the first and last names of each employee's dependents, along with their gender, and birthdate could result in identity theft and/or fraud.* *Release of the first and last names of the dependents of each dependent, along with their gender, and birthdate, combined with the full name and home address of the related employee could result in physical harm, particularly to juvenile dependents.* In general, I agree with the Organization's assessment. A reasonable person would consider that the contact, identity, employment and insurance information at issue could be used to cause the harms of identity theft and fraud, as well as humiliation and embarrassment. I accept the Organization's assessment that some of the information could be used to cause physical harm. 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, *The release of employee demographic information could be used to cause the significant harms of identity theft and/or fraud and/or personal harm.* *Personal humiliation and reputational harm is less likely, but possible.* *The risk of harm is ongoing because [the vendor] could not recall the email and was not able to confirm from the unintended recipient that the email was deleted and not otherwise shared. Further, [the vendor] was unwilling to provide [the Organization] with the recipient email address, so [the Organization] could not attempt to contact the recipient.*

	The fact that the information was sent to a single recipient unknown to the sender may diminish the likelihood that the information has wound up in the possession of a bad actor. 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. However, the information was sent to an unknown third party's Hotmail account and the Organization was unable to recall or confirm the deletion or destruction of the information. Therefore, there is an ongoing risk of harm to the affected individuals.

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, identity, employment and insurance information at issue could be used to cause the harms of identity theft and fraud, as well as humiliation and embarrassment. I accept the Organization's assessment that some of the information could be used to cause physical harm. 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. However, the information was sent to an unknown third party's Hotmail account and the Organization was unable to recall or confirm the deletion or destruction of the information. Therefore, there is an ongoing risk of harm to the affected individuals.

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 (employees) in an email dated December 7, 2020 in accordance with the Regulation. The Organization is not required to notify these affected individuals again.

The Organization reported that direct notification was not be possible for the dependent's whose information was at issue, because... "the Organization does not have contact information for each employee's dependents."

Section 19.1(1) of the Regulation states that notification must "... be given directly to the individual", although section 19.1(2) says "... the notification may be given to the individual indirectly if the Commissioner determines that direct notification would be unreasonable in the circumstances."

Given the Organization's submissions, I accept that indirect or substitute notice as described by the Organization is reasonable in this case, where the Organization is unable to contact affected individuals directly.

Jill Clayton
Information and Privacy Commissioner