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	Keurig Canada Inc. (Organization)
Decision number (file number)	P2021-ND-073 (File #017547)
Date notice received by OIPC	April 30, 2020
Date Organization last provided information	April 30, 2020
Date of decision	March 9, 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 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 information involved in the incident includes email addresses and the fact that email recipients are customers of the Organization. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The personal information was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• On April 20, 2020, an "Order Alert" email was sent to customers of the Organization. The purpose of the email was to inform recipients they had been mistakenly charged twice for online purchases. • The Organization inadvertently entered email addresses in the "cc" line, rather than the "bcc" line. • The incident was discovered on April 22, 2020.

Affected individuals	The incident affected 578 of individuals in Canada, of which 75 are residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Requested that recipients delete the email and refrain from copying or distributing the personal information. • Provided guidance on how to recognize and avoid fraudulent emails impersonating the Organization. • Recommended that individuals secure accounts associated with the Organization. • Amended policies and procedures to include a checklist that is to be followed prior to sending "bulk emails." The checklist includes the requirement of a second review, from a different employee, of the email prior to sending.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on April 24, 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 reports: *There is a small risk that a person could use this incident as an opportunity to send emails purporting to be from [the Organization] in an attempt to defraud those individuals.* *Also, because email addresses serve as usernames on Keurig.ca, there is a very small risk that a hacker could attempt to use an email address to gain access to another person's Keurig.ca account.* In my view, a reasonable person would consider that email addresses, particularly in conjunction with knowledge that the affected individuals are customers of the Organization, could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. It appears the information could also be used to potentially compromise other online accounts. 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 reports: *The likelihood of [harm] occurring is low, given the relatively small number in each of the two groups of recipients of the Order Alert Email, and the fact [the Organization] knows the identity of every person who received the Order Alert Email.* *[Risk] is very low because a person would also need a Keurig.ca user's password in order to access their account.*

	Keurig.ca is unlikely to be a target for hackers given the relatively limited amount of non-sensitive information that resides in a Keurig.ca account. For example, a hacker would not have access to a user's full credit card information. *It is our position that neither risk presents a "real risk of significant harm."* In my view, the likelihood of harm resulting from this incident is decreased as the personal information was compromised due to human error and not malicious intent. The "small number in each of the two groups of recipients" and "the fact that [the Organization] knows the identity of every person," who received the email may also reduce the likelihood of harm resulting from this incident; however, the Organization did not indicate whether all instances of the email were deleted, and, it is not possible for the Organization to ensure the personal information will not be used or disclosed further.

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 email addresses, particularly in conjunction with knowledge that the affected individuals are customers of the Organization, could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. It appears the information could also be used to potentially compromise other online accounts. These are significant harms.

The likelihood of harm resulting from this incident is decreased as the personal information was compromised due to human error and not malicious intent. The "small number in each of the two groups of recipients" and "the fact that [the Organization] knows the identity of every person," who received the email may also reduce the likelihood of harm resulting from this incident; however, the Organization did not indicate whether all instances of the email were deleted, and, it is not possible for the Organization to ensure the personal information will not be used or disclosed further.

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 by email on April 24, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner