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	Maplebear Inc., dba Instacart (Organization)
Decision number (file number)	P2020-ND-100 (File #017148)
Date notice received by OIPC	August 20, 2020
Date Organization last provided information	September 2, 2020
Date of decision	September 17, 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, • email address, • telephone number, • driver's license number, and • thumbnail image of driver's license. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies. With respect to some of the information at issue, the Organization reported that it "...could be considered business contact information". "Business contact information" is defined in section 1(1)(a) of PIPA to mean "an individual's name, position name or title, business telephone number, business address, business e mail address, business fax number and other similar business information."

	Section 4(1)(d) of PIPA says that the Act does not apply to the collection, use and disclosure of business contact information "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." In this case, I considered that the possible unauthorized access to the information was not "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." As a result, PIPA applies in this case.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On July 9, 2020, the Organization identified evidence that employees of its service provider accessed more "shopper profiles" than should have been necessary to perform their job. Shoppers are independent contractors on the Organization's technology platform, who provide shopping services on behalf of the Organization's customers. • The accesses occurred on or about June 5, 2020 and July 9, 2020. • The Organization reported that it does not have evidence that its shopper information was stored or exported.
Affected individuals	The incident affected 62 individuals, of which 6 are residents of Alberta.
Steps taken to reduce risk of harm to individuals	• The service provider terminated the employees from working on behalf of the Organization. • Provided direct notice to the impacted shoppers by email and offered free credit and identity protection product for 24 months. • Reported the incident to privacy regulators.
Steps taken to notify individuals of the incident	Affected individuals were notified in writing on August 19, 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	The Organization reported "...given the sensitivity of the information that was potentially accessed, [the Organization] considers that affected shoppers could be at risk of identity theft or fraud as a result of this incident."

important, meaningful, and with non-trivial consequences or effects.	In my view, a reasonable person would consider that the contact and identity (driver's license number and image of driver's license) information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. 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 it "… does not have any evidence that this information was exfiltrated, copied or stored by the vendor employees." In my view, a reasonable person would consider that the likelihood of identity theft and fraud resulting from this incident is increased because it resulted from deliberate action (unauthorized access). Although the Organization reported that the information was not exfiltrated, copied or stored, it did not rule out the possibility that the unauthorized parties viewed, read, or physically copied the affected individuals' personal information.

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 and identity (driver's license number and image of driver's license) information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are significant harms.

The likelihood of identity theft and fraud resulting from this incident is increased because it resulted from deliberate action (unauthorized access). Although the Organization reported that the information was not exfiltrated, copied or stored, it did not rule out the possibility that the unauthorized parties viewed, read, or physically copied the affected individuals' personal information.

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 that affected individuals were notified in writing on August 19, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner