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	DoorDash, Inc. (Organization)
Decision number (file number)	P2022-ND-058 (File #027143)
Date notice received by OIPC	August 24, 2022
Date Organization last provided information	September 27, 2022
Date of decision	September 30, 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 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 a U.S.-based technology company that connects consumers with restaurants, convenience stores, grocery stores, and retailers. The Organization uses an external service provider, Alorica, Inc. ("Alorica"), in connection with its customer service function. Customer support agents employed by Alorica have access to the Organization's internal customer service tools via their personalized user accounts. 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: Customers • name and • email address. Customers or Customers of Canadian merchants • name, • phone number, • delivery address, • email address,

	• basic order information, and • partial payment card information (i.e. card type and last 4 digits of card number). Delivery Drivers ("Dashers") • name, • email address, and • phone number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The Organization reported the personal information of 27, 453 affected individuals was collected in Alberta. With respect to Dashers, the Organization collected the personal information from the Dashers themselves in connection with their relationship to the Organization as independent contractors. With respect to consumers who are the Organization's customers, the Organization collected the personal information from the consumers themselves via the DoorDash app and website that DoorDash customers use to create accounts and place orders. With respect to consumers who are customers of merchants to whom the Organization provides platform services, the Organization collected the personal information on behalf of the merchant via the merchant's website or app, or via a website that the Organization operates for the merchant.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• On July 31, 2022, the Organization noticed suspicious access to a customer service tool from two Alorica user accounts. • The Organization promptly launched an investigation in conjunction with Alorica. • By August 5, 2022, suspicious activity originating from two additional Alorica user accounts was identified. • The investigation determined that the Alorica customer service agents provided their credentials to an unauthorized party in response to an apparent phishing scam. • The Organization reported "The unauthorized party was then able to access the relevant Organization customer service tools and run queries that returned certain information relating to customers and Dashers …"

	• The Organization believes the unauthorized access to personal information occurred between July 25 and August 2, 2022. • The advanced tactics used in this incident appear to be connected to a much wider phishing campaign that has been reported in the news as targeting a number of other technology companies.
Affected individuals	The Organization reported the following number of affected individuals: • 14, 867 customers. • 11,648 individuals who were either Canadian DoorDash customers or customers of Canadian merchants. • 938 Door Dash delivery drivers. The Organization also reported there was an additional subset of consumers that are customers of merchants to whom it provides platform services, where customers order directly from the merchant. The Organization did not provide the number of affected individuals in this subset.
Steps taken to reduce risk of harm to individuals	• Quickly disabled Alorica's access to the Organization's systems upon identifying the suspicious activity originating from the Alorica user accounts. The Organization did not reactivate Alorica's access until additional security measures were put in place. • Engaged a leading third-party forensic investigation firm to assist with its investigation. • Contacted U.S. law enforcement authorities. • Conducted additional phishing awareness security exercises for Organization personnel (notwithstanding the fact that the Organization's employees were not the target of the relevant phishing attack). • Worked closely with Alorica to ensure that Alorica enhances its security measures in response to this issue and is also further enhancing its own security measures.
Steps taken to notify individuals of the incident	Affected individuals were notified of the incident by email on August 25, 2022. The Organization also reported, *"In addition to the details set out above, DoorDash also identified a subset of consumers that are customers of merchants to whom DoorDash provides platform services, where the customers order directly from the merchant. One of these services is known as the "Drive" service where DoorDash delivers the order for the merchant, and another is the "Storefront" service where DoorDash builds the merchant's website on behalf of the merchant. DoorDash will be informing affected*

	merchants about this issue, or in some cases the intermediary middleware provider that facilitates the relationship between DoorDash and the merchant."
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 risk of harm to affected individuals is low; however, your Office has previously identified phishing as a possible harm that may result from the unauthorized access to email addresses.* In my view, a reasonable person would consider the name and email address, particularly when combined with brand affiliation and partial credit card number, could be used for phishing purposes 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, *Given the non-sensitive nature of the impacted personal information and the steps that DoorDash has taken to reduce the risk of harm, including notification to affected individuals, ... DoorDash believes that there is a low likelihood of harm that may result from this incident. There is no evidence to date that the affected information has been used for fraud or identity theft.* In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the incident appears to be the result of malicious actions. Further, the information may have been exposed for approximately 8 days. Although the Organization has adopted additional safeguards, these were not in place at the time of the breach. Further, this does not necessarily mitigate the potential harm that may result if the information accessed from the Organization's systems were to be used for fraudulent purposes. The Organization reported, "*There is no evidence to date that the affected information has been used for fraud or identity theft."* The lack of reported incidents resulting from this breach to date is not a mitigating factor. Phishing, identity theft and fraud can occur months and even years after a data breach.
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 name and email address, particularly when combined with brand affiliation and partial credit card number, could be used for phishing purposes increasing vulnerability to identity theft and fraud. These are significant harms.

The likelihood of harm resulting from this incident is increased because the incident appears to be the result of malicious actions. Further, the information may have been exposed for approximately 8 days. Although the Organization has adopted additional safeguards, these were not in place at the time of the breach. Further, this does not necessarily mitigate the potential harm that may result if the information accessed from the Organization's systems were to be used for fraudulent purposes. Despite the Organization's statement that there is no evidence to date that the affected information has been used for fraud or identity theft, the lack of reported incidents resulting from this breach to date is not a mitigating factor. Phishing, identity theft and fraud can occur months and even years after a data breach.

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 August 25, 2022, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance