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	Careem Inc. (Organization)
Decision number (file number)	P2019-ND-018 (File #008432)
Date notice received by OIPC	April 23, 2018
Date Organization last provided information	December 11, 2018
Date of decision	February 14, 2019
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: <u>Customers:</u> • name, • telephone number, • email address, • location, • trip history, and • hashed credit card information (number, expiry date and security code). <u>Captains (Drivers)*:</u> • name, • telephone number, • make and model of vehicle driven, • license plate number, • trip history, • bank number, • national ID number, and • driver's license.

	This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The Organization reported that it is unable to confirm exactly where the personal information of its Alberta customers was collected; however, it was likely collected outside of Alberta and in jurisdictions where the Organization operates. The Organization said that while it is possible to access the Organization's mobile application anywhere in the world, it seems unlikely that the personal information of the Organization's Alberta customers was actually collected in Alberta as the Organization's services cannot be used in Alberta. *The Organization reported that all drivers involved in the incident are based throughout the Middle East and North Africa and Pakistan. There are no drivers in Canada or Alberta. To the extent the personal information was collected in Alberta, I have jurisdiction in this matter.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On January 14, 2018, the Organization received an email from an unknown hacker claiming to have infiltrated its IT systems. The email demanded a ransom, which, if not paid, would result in the hacker disclosing the information publicly. • On January 25, 2018, the Organization paid the ransom. • The Organization investigated and determined that the hacker infiltrated its IT systems sometime in December 2017, and had both accessed and stolen the personal information of customers and drivers. • The Organization reported there is a possibility the hacker exfiltrated part or all of the Organization's source code. • The Organization said it does not store credit card information on its systems, but it did maintain a token, a one-way hash of card number, as a fraud prevention mechanism. • The Organization believes that there is no realistic risk of reconstituting credit card number and expiry dates since the cost of the computational power required to brute force significantly outweighs the black market price for a credit card number.
Affected individuals	The incident affected 1,039 individuals residing in Alberta.

Steps taken to reduce risk of harm to individuals	• Retained a cybersecurity firm to investigate the scope and cause of the incident and to strengthen IT security infrastructure. • Notified all affected customers and drivers. • Notified insurers and applicable law enforcement agencies. • Implementing new IT security policies including an IT Security SteerCo for decision-making. • Hired a Chief Information Technology Security Officer. • Retained a global IT security firm to undertake a compromise assessment test.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on April 23, 2018.
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 personal information of customers may potentially be used to conduct identity theft and/or fraud. However, it would be extremely difficult and very unlikely to use a customer's name in conjunction with their phone number, and/or e-mail address to conduct identity theft and subsequently fraud of those individuals". The Organization also said "… there is a potential security/safety risk to those individuals to the extent a customer took re-occurring trips or used the same locations for pick-up/drop-off point as the future location of that customer may be known or able to be predicted, thereby potentially presenting a safety risk to that individual," and noted a remote possibility that an attacker could reconstitute a credit card number and expiry date to cause financial harm. I agree with the Organization's assessment. A reasonable person would consider that, particularly when combined with profile information (e.g. information that individuals are customers of the Organization), individual names, mobile telephone numbers and email addresses of customers could be used to send sophisticated, user-specific emails and text messages purportedly from the Organization (phishing, smishing or SMS/text phishing). Merely clicking on a link, without a user providing any additional information, could potentially cause significant harm (e.g. activate malware, infect users' computer/networks). Further, as smartphones are one of the primary means to access the Organization's services, the Organization's users may be particularly vulnerable to these types of harms, as well as identity theft and fraud. I also agree with the Organization that there is a potential security/safety risk.

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 "The likelihood that identity theft/fraud would occur to any of the 1039 Alberta customers (excluding those whose hashed credit card information was disclosed) is very low and virtually zero. It would be extremely difficult to conduct identity theft of an individual using that individual's name, phone number, and/or email address especially since an individual's phone number is public information in many instances." The Organization reported that "For credit card customers, the risk of fraud and identity theft is very low to virtually zero" because of the knowledge and computational power that would be required to reconstitute a credit card number. As well, the Organization said, "it is not possible to reconstitute the three digit credit card security code using the source code thereby reducing the chance of fraud/identity theft as a result of the disclosure of credit card information." The Organization said that "of the 1039 Alberta residents affected by the incident, only 35 Alberta customers held credit cards on file with [the Organization]." The Organization also reported that "The risk of a security/safety risk to customers as a result of previous trip information and saved locations of customers being accessed by the Hacker is low to moderate. Such a risk would only exist to the extent a customer took re-occurring trips using the same route on a pattern of times/dates and where those previous trips and/or locations could be used to predict the future location of customers." Finally, the Organization said, "To date, [the Organization] is not aware of any instances of any personal information of customer or captains being used by the Hacker or third parties." In my view, the likelihood of significant harm resulting from this incident is increased because the personal information was compromised due to a deliberate unauthorized intrusion by a third party. The Organization reported that the hacker had already both accessed and stolen the personal information of customers and drivers. Further, the Organization can only assume that the cost of reconstituting the credit card information would be prohibitive for the hacker. Finally, the lack of reported incidents resulting from this breach to date is not a mitigating factor, as phishing/smishing, 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.	

A reasonable person would consider that, particularly when combined with profile information (e.g. information that individuals are customers of the Organization), individual names, mobile telephone numbers and email addresses of customers could be used to send sophisticated, user-specific emails and text messages purportedly from the Organization (phishing, smishing or SMS/text phishing). Merely clicking on a link, without a user providing any additional information, could potentially cause significant harm (e.g. activate malware, infect users' computer/networks).

Further, as smartphones are one of the primary means to access the Organization's services, the Organization's users may be particularly vulnerable to these types of harms, as well as identity theft and fraud. I also agree with the Organization that there is a potential security/safety risk.

The likelihood of significant harm resulting from this incident is increased because the personal information was compromised due to a deliberate unauthorized intrusion by a third party. The Organization reported that the hacker had already both accessed and stolen the personal information of customers and drivers. Further, the Organization can only assume that the cost of reconstituting the credit card information would be prohibitive for the hacker. Finally, the lack of reported incidents resulting from this breach to date is not a mitigating factor, as phishing/smishing, 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 in an email dated April 23, 2018 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner