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	Skip The Dishes Restaurant Services Inc. (Organization)
Decision number (file number)	P2020-ND-020 (File #013677)
Date notice received by OIPC	August 23, 2019
Date Organization last provided information	August 23, 2019
Date of decision	February 14, 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 the 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 the following information: • first and last name, • email address, • telephone number, • address, • driver's licence, vehicle insurance and vehicle registration, • work eligibility documents (e.g. permanent residency card, birth certificate, passport, work/study permit, social insurance card), • bank deposit information (account holder name, transit number, institution, account number), and • credit card number, expiry month and year, CVV. 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	• Unknown individual(s) used credential stuffing to gain access to the Organization's courier accounts accessible through its "Courier Portal". "Credential Stuffing" is the process by which an attacker steals or purchases username and password combinations (possibly on the dark web) and enters those credentials on websites to see if they can gain access. • The incident occurred on July 11, 2019 and was discovered the same day when the Organization's security operations team detected an unusually high number of failed logins on the Courier Portal.
Affected individuals	The incident affected 4 individuals in Alberta.
Steps taken to reduce risk of harm to individuals	Adding two factor authentication to login into the Courier Portal and to make any changes to email, password and banking information within the Courier Portal.
Steps taken to notify individuals of the incident	Affected individuals were notified by telephone and email on August 12, 2019.
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 possible harms include "Identity Theft, fraud and financial loss for the impacted couriers". I accept the Organization's assessment. A reasonable person would consider that the contact, identity, employment and financial information at issue could be used to cause the harms of identity theft, fraud and financial loss. Email address 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 "If the intruders accessed the accounts with the intention of accessing, copying, etc the personal information of the courier, then there is a likelihood of potential harm to the courier such as fraud, identity theft and/or financial loss. However, the intention of the intruder remains unknown". 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 action (credential stuffing). The intention of the unauthorized parties is not known.
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 financial information at issue could be used to cause the harms of identity theft, fraud and financial loss. Email address 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 action (credential stuffing). The intention of the unauthorized party(s) is not known.

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 affected individuals were notified by telephone and email on August 12, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner