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	SkipTheDishes Restaurant Services Inc. (Organization)
Decision number (file number)	P2020-ND-102 (File #017146)
Date notice received by OIPC	August 19, 2020
Date Organization last provided information	August 19, 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, • telephone number, • email address, • delivery address, • order history, and • first 4 digits and last 4 digits of credit card saved to the account. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta via the Organization's website and/or application.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On July 22, 2020, the Organization's third-party account takeover and fraud analysis vendor notified the Organization of an unusual pattern of activity. • The Organization investigated and discovered a malicious actor performed a credential-stuffing attack by testing breached email and password combinations that were obtained outside of the Organization • The Organization estimates that approximately 160 Alberta accounts were affected by this vulnerability between April 2020 and July 31, 2020.
Affected individuals	The incident affected 160 individual accounts in Alberta.
Steps taken to reduce risk of harm to individuals	• Secured customer accounts by resetting passwords. • De-linked social media merged accounts. • Revoked tokens. • Provided education on good password practices. • Implemented mechanism to ensure social merge function can no longer be used to perform credential stuffing attacks.
Steps taken to notify individuals of the incident	Affected individuals were notified of the incident on August 18, 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's notification to affected individuals said "You should remain vigilant for any unusual use of your online accounts or suspicious communications from third parties pretending to be [the Organization]". In my view, a reasonable person would consider the contact and transaction information (order history) at issue, particularly when combined with email address, could be used for phishing purposes, increasing vulnerability to identity theft and fraud. Confirmed valid credentials could be used to compromise 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 did not specifically provide an assessment of the likelihood that significant harm would result from this incident, although it reported that "…there is little doubt that the account takeovers are being perpetrated by malicious third party attackers" and "…in totality there may be a real risk of significant harm to the affected individuals." 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). Further, the information may have been exposed for approximately 4 months.

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 the contact and transaction information (order history) at issue, particularly when combined with email address, could be used for phishing purposes, increasing vulnerability to identity theft and fraud. Confirmed valid credentials could be used to compromise online accounts. 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). Further, the information may have been exposed for approximately 4 months.

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 on August 18, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner