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)	P2021-ND-243 (File #020723)
Date notice received by OIPC	April 22, 2021
Date Organization last provided information	November 16, 2021
Date of decision	December 1, 2021
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 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 April 5, 2021, the Organization learned of suspicious activity on its network. • The Organization investigated and found a small number of instances where fraudsters were bypassing two-factor authentication (2FA) by chatting with agents, posing as customers and requesting that account telephone numbers be changed. • In most cases, the fraudster was able to supply the original telephone number on the account, as well as the customer's email address and, in some cases, a delivery address. It is likely that the fraudster obtained this information from breaches that occurred on other websites, outside of the Organization's environment. • After changing account telephone numbers, fraudsters were able to gain access to the accounts. • The incidents occurred from August 2020 to March 2021, with the majority occurring in March 2021.
Affected individuals	The incident affected 38 individual accounts in Alberta.
Steps taken to reduce risk of harm to individuals	• Reset customer account passwords to a random, unpredictable one. • Sent an email to customers notifying them that there has been unusual activity on their account, and requiring them to choose a new password. • Blocked all phone numbers used by the fraudster. • Updated processes and took steps to provide additional training to agents to ensure customer support staff recognize the importance of asking proper verification questions.
Steps taken to notify individuals of the incident	Affected individuals were notified of the incident on April 22, 2021.
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, *…we identified that an unknown third party may have accessed or attempted to gain access to your customer account by using personal information obtained from unknown and unidentifiable third party sources…You may have already received an email notifying you of this activity, and the steps we have taken to secure your account, including locking your account and sending a password reset….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 and telephone numbers, could be used for phishing or to impersonate customers, 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 reported, *The personal information available … is of a lower degree of sensitivity. However, given that the customer's information has already been breached elsewhere, outside of [the Organization's] environment, there may be a real risk of significant harm to the affected individuals.* I agree with the Organization's assessment. 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 7 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 and telephone numbers, could be used for phishing or to impersonate customers, 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 actions. Further, the information may have been exposed for approximately 7 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 by email on April 22, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner