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-034 (File #013790)
Date notice received by OIPC	November 7, 2019
Date Organization last provided information	December 4, 2019
Date of decision	March 9, 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 headquartered in Winnipeg, and 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, • delivery address, • email address, • telephone number, and • order history. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• In mid-2019, the Organization's customer service department noticed an increased in "account takeover" complaints from consumers. These complaints involved concerns that unauthorized orders were being placed in customer accounts.

	• The Organization investigated and found the account takeovers occurred as a result of individuals having lost control of their passwords through a combination of many factors. The Organization did not uncover a failure of security safeguards under the Organization's control or a compromise of its systems. • Nonetheless, as a result, unauthorized users may have accessed limited personal information that account holders entered in setting up an account.
Affected individuals	The Organization reported approximately 2,400 individual accounts in Alberta may have been affected.
Steps taken to reduce risk of harm to individuals	• Has a robust existing information security program. • Taking additional steps to detect and thwart such incursions. • Enhancing existing tools, blocking traffic, and engaging in proactive threat detection. • Adding information to its website that provides education about good password hygiene and referring users to the government's getcybersafe.gc.ca website. • When a possible threat is detected, the Organization will reset the password to protect the users from potential harm and notify users of the reasons and provide a notification containing educational content re: password hygiene. • Advising consumers to reset password resets, remove credit card information and report fraudulent charges to their financial institution. • Identifying past users whom the investigation suggests might have lost control of their accounts and providing them notification by email with the same information.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on October 31, 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 that "… although the personal information available … is of a lower degree of sensitivity, when the account takeovers are viewed in the larger pattern of behaviour taking place outside [the Organization's] systems, there appears to be a real risk of significant harm to affected individuals, at least through the potential confirmation of address information that may already be in the hands of the malicious actors". 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." In my view, a reasonable person would consider the likelihood of harm resulting in this case is increased because the personal information was compromised due to the malicious action of unknown third party(s) (deliberate intrusion) who gained access to user accounts. The accounts may have been compromised for several 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 addresses, 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 in this case is increased because the personal information was compromised due to the malicious action of unknown third party(s) (deliberate intrusion) who gained access to user accounts. The accounts may have been compromised for several 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 October 31, 2019 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner