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	Sustainable Produce Urban Delivery, Inc. (Organization)
Decision number (file number)	P2021-ND-055 (File #016613)
Date notice received by OIPC	August 4, 2020
Date Organization last provided information	August 4, 2020
Date of decision	March 9, 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, • driver's license, • social security number, • address, • telephone number, and • salary. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization reported "(Likely) a phishing attack that enabled a 3rd party access to set up an email forwarding rule." • The incident occurred between June 16, 2020 and July 8, 2020.

	• The incident was discovered by a vendor on July 8, 2020. The Organization stopped the forwarding of email immediately. • On July 14, 2020, the Organization also disabled the ability to forward email from any email Spud.ca account. • The Organization reported that approximately 150 emails were affected, and not all emails had relevant information.
Affected individuals	The incident affected 300 individuals of which one hundred (100) were residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Blocked email forwarding rules. • Completed forensic analysis and confirmed threat is eliminated. • Added security and protection. • Added education and communication regarding cyber-training security.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on July 28, 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 reported that the possible harms that may occur as a result of the breach are "Unknown, identity theft." In my view, a reasonable person would consider that the contact, identity and employment information at issue could be used to cause the significant harms of identity theft, fraud and financial loss.
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 likelihood that the significant harm will result is "Unknown". In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). Further, the intruder appears to have had access to the information over the course of three (3) weeks.
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 and employment information at issue could be used to cause the significant harms of identity theft, fraud and financial loss. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). Further, the intruder appears to have had access to the information over the course of three (3) weeks.

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 July 28, 2020. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner