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	Fat Face Ltd. (Organization)
Decision number (file number)	P2021-ND-211 (File #020241)
Date notice received by OIPC	March 23, 2021
Date Organization last provided information	March 23, 2021
Date of decision	November 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 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's head office is in Hampshire, UK. 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: • name, • email address, • combination of telephone number and/or address (in some cases multiple, if multiple transactions), • payment method, • last 4 digits of card number (the rest being masked), • payment card expiry date, and • basic order details. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On January 17, 2021, the Organization identified suspicious activity within its IT systems. • An investigation determined that unidentified threat actors gained access to certain systems during a limited period of time from December 25, 2020. • On January 18, 2021, the Organization contained the incident and began reviewing and categorizing the data potentially involved in the incident. • On March 9, 2021, the Organization determined that there are a number of customers in the database tables that appear to be located in Canada, including in Alberta.
Affected individuals	The incident affected 800,000 individuals, including 318 Canadians, of which 53 are Alberta residents.
Steps taken to reduce risk of harm to individuals	• Investigated with assistance of third-party security specialists, and identified affected individuals and information involved. • Worked with authorities and external security experts to ensure a comprehensive response to the incident. • Reported the incident to data protection and law enforcement authorities as well as the Action Fraud and the National Cyber Security Centre • Used containment measures to identify potentially malicious activity linked to the incident and monitoring deep and dark web attacker "leak sites". • Offered affected individuals an identity-monitoring product upon request. • Intending to take additional steps to further strengthen the systems security.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on March 23, 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 reported, *While the organization assesses the likelihood of harm as low, the individuals involved may be subject to phishing attempts or unsolicited communications.* In my view, a reasonable person would consider that the contact and transaction information, along with email addresses, could be used for the purposes of phishing, 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, *As the information involved is essentially limited to contact information with only partial credit card information, the likelihood of harm is assessed as low. The individuals involved are notified to further reduce this likelihood*. In my view, a reasonable person would consider 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). Although the Organization has put additional safeguards in place, these were not in place at the time of the breach. Further, this does not necessarily mitigate the potential harm that may result if the information were to be used for fraudulent purposes. Finally, the information may have been exposed for 25 days.

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 and transaction information, along with email addresses, could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are significant harms.

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). Although the Organization has put additional safeguards in place, these were not in place at the time of the breach. Further, this does not necessarily mitigate the potential harm that may result if the information were to be used for fraudulent purposes. Finally, the information may have been exposed for 25 days.

I require the Organization to notify the affected individuals whose 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 letter on March 23, 2021 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner