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	Aeroplan Inc. (Organization)
Decision number (file number)	P2021-ND-063 (File #013556)
Date notice received by OIPC	October 23, 2019
Date Organization last provided information	November 11, 2019
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"	Aeroplan Inc. is a wholly owned subsidiary of Air Canada. They are separate entities. Air Canada is responsible for handling potential breaches of privacy for Aeroplan Inc. 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, • gender, • date of birth, • email address, • home address, • telephone number, and • additional customer information. 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.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On September 17, 2019, malicious actor(s) used valid credentials obtained from prior breaches unrelated to the Organization to access the some customer accounts. • The incident was a remote cyber attack against a cloud based authentication service. • Using Application Programming Interface (API) calls, the attackers used the previously exposed email address and password to log in, change the password, and then change the email address on file to an invalid email address. • The breach was discovered on September 17, 2019 when customers who received an automated email notice that a change was made to their account, contacted the Organization.
Affected individuals	The incident affected 7,500 accounts, of which approximately 700 belong to Albertans.
Steps taken to reduce risk of harm to individuals	• Inactivated accounts that were suspected of being compromised to prevent any further exposure. • Re-activated the accounts and at sign-in guided the customer through a password reset process. • Flagged all affected accounts for heightened monitoring of potentially fraudulent activity. • Described the steps taken to reduce the risk of a similar event occurring in the future. • Enhanced other IT safeguards to prevent reoccurrence.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on October 23, 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 "The information could be used for phishing." I agree with the Organization's assessment. A reasonable person would consider email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. Contact and identity information (name and date of birth) could also be used for identity theft and fraud. These are all 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 "There is a risk the information could be used for phishing but we an unable to assess the likelihood. At this stage, we are unaware of any harm to individuals." 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).

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 email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. Contact and identity information (name and date of birth) could also be used for identity theft and fraud. These are all 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).

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 23, 2019 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner