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	Apple Canada Inc. (Organization)
Decision number (file number)	P2018-ND-134 (File #009751)
Date notice received by OIPC	October 11, 2018
Date Organization last provided information	October 11, 2018
Date of decision	October 16, 2018
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify individuals whose 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)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • first name, • last name, • home address, • email address, • telephone number, and • last four digits of the user's stored payment card (if a payment card was on file). 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 in this matter.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• An external party may have phished one of the Organization's employee's credentials and queried the central system that stores iTunes customer account information. • The Organization reset the credentials used by the external party upon discovery of this incident, thereby terminating the external party's ability to access the system containing iTunes customer account information. • The third party was able to access the account information for 2 individuals in Alberta prior to the termination of their access to the system. • Internal monitoring tools detected suspicious activity in the central system and these alerts were quickly escalated for response and review. • The incident occurred on September 14, 2018 and was discovered the same day.
Affected individuals	The incident affected 1,720 customers, including 2 individuals in Alberta.
Steps taken to reduce risk of harm to individuals	• Contacted the data subjects to remind them to use the Organization's tools to protect their accounts. • Reminded data subjects to be vigilant against phishing attempts, and to not disclose their online account passwords or similar information by email or text message. • The Organization will continue to provide ongoing training and awareness reminders to employees to help them identify and avoid phishing attacks, as that was the attack vector used by the bad actors in this instance. • Reported incident to the Federal Bureau of Investigation.
Steps taken to notify individuals of the incident	Affected individuals were notified by email sent October 3, 2018.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the 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 primary harm that could occur as a result of this incident is an increase in phishing attempts." I agree with the Organization's assessment. The contact information, and particularly email address, could be used for phishing purposes. Previous breach notification decisions issued by my office have found phishing to be a significant harm.

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.	In assessing the likelihood of harm resulting from this breach, the Organization reported "We have no specific evidence to show that the bad actors plan to use the data in question for phishing. Therefore, we believe there is a moderate likelihood of phishing attempts as a result of the incident. However, the risk of successful phishing is mitigated by the reminders we have provided to customers in our notification to remain vigilant, as well as by the ongoing work the company does to ensure customers are aware of their security choices (including the availability of two factor authentication). As a result, we believe that this risk is overall best characterized as low to moderate." In my view, the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (phishing). The Organization can only speculate as to the intentions of the unauthorized actor(s).

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 as a result of this incident.

The contact information, and particularly email address, could be used for phishing purposes. Previous breach notification decisions issued by my office have found phishing to be a significant harm. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (phishing). The Organization can only speculate as to the intentions of the unauthorized actor(s).

I require the Organization to notify any affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand that affected individuals were notified by email sent October 3, 2018. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner