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 Inc. (Organization)
Decision number (file number)	P2018-ND-35 (File #007303)
Date notice received by OIPC	December 7, 2017
Date Organization last provided information	February 13, 2018
Date of decision	February 28, 2018
Summary of decision	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify the individual 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, • billing address, • credit card number, • credit card expiration date, and • credit card verification value. This information is about an identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected via the Organization's online store.
DESCRIPTION OF INCIDENT	
☒ loss ❑ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On November 15, 2017, an employee with the Organization's service provider attempted to misuse the personal information of an Alberta resident, who is a customer of the Organization.

	• The service provider's employee in question attempted to make an unauthorized purchase using the customer's credit card information. • The Organization identified the fraudulent activity and canceled the order.
Affected individuals	The incident affected one (1) Alberta resident.
Steps taken to reduce risk of harm to individuals	• Terminated the employee who misused the Organization's customer information. • Monitoring for suspicious incident by both the service provider and the Organization. • Tried to notify affected individual and advise him to be diligent in monitoring for unauthorized charges. • Require reasonable physical and data security practices of its vendors with access to any customer information. • Notified law enforcement.
Steps taken to notify individuals of the incident	Two attempts using different couriers were made to deliver the notification to the affected individual (on December 6, 2017 and January 10, 2018); however, each time, the letter was returned to the Organization after the individual failed to pick it up as instructed. The Organization does not have an email address for the affected individual.
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 "It is possible that fraudulent credit card purchases using the individual's credit card could result from this incident. If the individual's card is replaced by the issuer, the individual may not be able to make use of his credit card for a short period of time." In my view, the identity and the financial information at issue could be used to cause the significant harms of fraud, financial loss and identity theft.
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 that "(b)ased on the information involved, and the swift actions of [the Organization and the service provider], we believe that the risk of actual harm to the affected Alberta resident is likely very low in light of the fact that we caught the fraudulent activity and stopped it. However, because there is some risk that the former contractor could attempt to again make use of the customer's credit card information, we have notified the affected Alberta resident and encouraged him to continue to be diligent in watching for unauthorized charges made with the payment card and to quickly report any suspicious activity to the

	card issuer. While our investigation continues, neither [the Organization] nor [the service provider] is aware of any subsequent fraud involving the Alberta resident's information nor any financial loss or other harms attributable to this incident. In general, major credit card companies have rules in place that restrict them from requiring cardholders to pay fraudulent charges that are timely reports. Also the now-terminated employee does not have any continuing access to the information affected." In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a third party (deliberate misuse of information). The Organization can only speculate that the affected individual will not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud.

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 individual.

The identity and the financial information at issue could be used to cause the significant harms of fraud, financial loss and identity theft. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a third party (deliberate misuse of information). The Organization can only speculate that the affected individual will not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud.

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

I understand the Organization made reasonable attempts to notify the affected individual by letters couriered on December 6, 2017 and January 10, 2018 in accordance with the Regulation. The Organization is not required to make further attempts to notify the affected individual.

Jill Clayton
Information and Privacy Commissioner