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	OnePlus Technology Co., Ltd. (Organization)
Decision number (file number)	P2018-ND-042 (File #007945)
Date notice received by OIPC	February 28, 2018
Date Organization last provided information	February 28, 2018
Date of decision	March 5, 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 those individuals 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 Organization reported that "the potentially compromised data included customers' credit/debit card numbers, credit/debit card expiration dates, and CVV/CSC numbers. Our investigation to date has found no evidence that any other data elements, such as customer name, were compromised during the incident." This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected via the Organization's website payment page.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On January 11, 2018, customers of the Organization reported experiencing suspected credit card fraud and believed that their purchases from OnePlus.net were potentially related to the fraudulent credit card activity. • The Organization investigated, and found that an unknown attacker had injected a malicious script into the payment processing page of the Organization's website.

	• The malicious script intermittently captured credit card information entered by customers on the payment page during the period between November 21, 2017 and January 11, 2018.
Affected individuals	The incident potentially affected 3,928 Canadians, including 485 Albertans.
Steps taken to reduce risk of harm to individuals	• Quarantined the affected server, did a security scan to patch vulnerabilities, and suspended website credit card payments. • Reviewed and confirmed the security of a new proposed integration method before reinstating credit card payments for the website. • Engaged an expert cybersecurity firm to assist with reinforcing the security of systems. • Reported the incident to Hong Kong law enforcement. • Notified customers through a OnePlus.net forum post on January 19, 2018. • Providing affected Canadians with no cost credit/identity monitoring for one year.
Steps taken to notify individuals of the incident	Affected individuals were notified by email sent January 19, 2018 and a more detailed notification letter was sent to potentially affected residents of Canada on February 12, 2018.
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 "…due to the potential compromise of payment card data, certain customers may face an increased risk of fraudulent credit/debit card charges." I agree with the Organization. The financial information at issue could be used for the significant harms of identity theft and fraud.
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 did not specifically assess the likelihood of harm resulting from this incident, but said "Out of an abundance of caution, we have notified all customers who entered their card data on our payment page during the window of time in which the malicious script is believed to have been active." 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 an unknown third party (deliberate intrusion). The information may have been exposed for a month and a half.

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. The financial information at issue could be used for the significant harms of identity theft and fraud. 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). The information may have been exposed for a month and a half. The Organization is required to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand affected individuals were notified by email sent January 19, 2018 and a more detailed notification letter was sent to potentially affected residents of Canada on February 12, 2018. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner