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	OneStopParking (Organization)
Decision number (file number)	P2015-ND-50 (File #000511)
Date notice received by OIPC	March 24, 2015
Date Organization last provided information	August 17, 2015
Date of decision	August 18, 2015
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 runs an e-commerce website that provides parking services at airport hotels and seaports. It does not have any physical stores/locations. I have jurisdiction because 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, • address, • credit card number and expiration date, and • CVV code. This information is "personal information" as defined in section 1(1)(k) of PIPA and was collected from Alberta residents via the Organization's website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On December 25, 2015, a security blogger alerted the Organization to a potential website compromise. • The Organization initiated an internal investigation and found a website vulnerability. The investigation determined that the personal information of customers who used the Organization's website between August 1, 2014 and December 31, 2014 may have been accessed by an unauthorized individual(s).
Affected individuals	The Organization is unable to confirm exactly how many individuals may have been affected, but estimates approximately 21,700; of these, approximately 40 are Albertans.
Steps taken to reduce risk of harm to individuals	• The server was immediately shut down. • Initiated internal investigation. Retained independent forensic investigators to assist. Identified a code vulnerability, which was fixed. Deployed sophisticated software to monitor all traffic. • Offered 1 year free credit monitoring and fraud resolution services to affected individuals.
Steps taken to notify individuals of the incident	Affected individuals were notified in a letter sent on March 17, 2015.
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 did not explicitly identify any harm that could be caused as a result of this incident, but reported that it "is providing each customer with information on how to protect against identity theft and fraud." In my view, the personal information involved is sensitive. The types of harm that could result from unauthorized access to the personal information in this instance are identity theft and fraud. In my view, 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 did not explicitly state its assessment of the likelihood of harm resulting from this incident. However, it reported that it is unable to determine exactly which individuals may have been affected by the code vulnerability, or exactly what information may have been accessed. The Organization advised that some fraudulent credit card activity was reported, but there is no evidence to tie that activity to this incident. In my view, the likelihood of harm resulting from this incident is increased because of the malicious intent, the length of time

	the personal information may have been exposed (5 months), and the number of individuals whose information may have been accessed.

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 types of harm that could result from this incident are identity theft and fraud, which are significant harms. The likelihood of harm resulting from this incident is increased because of the malicious intent, the length of time the personal information may have been exposed (5 months), and the number of individuals whose information may have been accessed.

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

I understand that the Organization notified the affected individuals in a letter sent on March 17, 2015. Therefore, the Organization is not required to notify the individuals again.

Jill Clayton
Information and Privacy Commissioner