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	Park 'N Fly (Organization)
Decision number (file number)	P2016-ND-06 (File # 000719)
Date notice received by OIPC	April 24, 2015
Date Organization last provided information	April 24, 2015
Date of decision	February 9, 2016
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)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • telephone number, • email address, • passwords, • billing address, • credit card number, • credit card expiration date, • credit card verification code (CVV) 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 online ecommerce application.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization's ecommerce application was compromised between November 27, 2013 and December 24, 2014. • At the time of the compromise, the ecommerce application processed customers' online payments. • Personal information of individuals whose payments were processed between November 27, 2013 and December 24, 2014 may have been compromised. • The incident was discovered in September 2014 and was contained sometime between December 24, 2014 and January 13, 2015.
Affected individuals	Five (5) Alberta residents were affected by the incident.
Steps taken to reduce risk of harm to individuals	• The Organization contracted a third party forensics firms to conduct an investigation into the incident. • A free 12-months credit monitoring was provided to affected individuals by the Organization. • The Organization provided information on identity theft and fraud protection to customers on its website. • Payment processing via the Organization's ecommerce website was discontinued and replaced by PayPal payment processing. • Malicious software installed on the ecommerce site by unauthorized users were identified and removed. • Enhance security controls have been implemented to protect the Organization's ecommerce site. • A toll-free line was set up to assist customers who needed more information about the incident.
Steps taken to notify individuals of the incident	• Notifications to affected individuals were carried out between January 13, 2015 and February 27, 2015. • The Organization also issued a number of media updates on the incident. • Written notifications to Alberta residents were mailed on February 27, 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 it is providing customers with "information on this security compromise and protection against identity theft and fraud." In my view, the personal information involved sensitive identity and financial information. The types of harm that could result from unauthorized access to the personal information in this instance are identity theft and fraud. 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 assess the likelihood of harm resulting from this incident, however it reported it "has reason to believe the intruder stole some data from certain payment cards." In my view, the likelihood of harm resulting from this incident is increased because the personal information was accessed by unauthorized individuals with malicious intent. Also, the personal information at issue may have been exposed for over 13 months.

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 personal information involved sensitive identity and financial information that could be used to cause the significant harms of identity theft and fraud. The information was accessed by unauthorized individuals with malicious intent. Also, the personal information at issue may have been exposed for over 13 months.

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

I understand the Organization notified the affected individuals in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner