



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	LuckyPet, Inc. (Organization)
Decision number (file number)	P2016-ND-29 (File #002843)
Date notice received by OIPC	April 29, 2016
Date Organization last provided information	April 29, 2016
Date of decision	July 21, 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 <i>Personal Information Protection Act</i> (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”	<p>The incident involved all or some of the following information:</p> <ul style="list-style-type: none">• name,• email address,• shipping address, and• credit card information, including expiry date and security code). <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA. Some of the information was collected in Alberta.</p>
DESCRIPTION OF INCIDENT	
<input type="checkbox"/> loss <input checked="" type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	

<p>Description of incident</p>	<ul style="list-style-type: none"> • On approximately October 12, 2015, an unknown and unauthorized party exploited a vulnerability in the Organization’s third-party shopping cart software used on its website and inserted malicious software that intercepted information provided by customers making purchases. • The Organization’s website contractor discovered the malicious code on March 16, 2016.
<p>Affected individuals</p>	<p>The incident affected 148 residents of Alberta.</p>
<p>Steps taken to reduce risk of harm to individuals</p>	<ul style="list-style-type: none"> • The malicious code was removed. • The Organization updated its software, and was informed that the vulnerability was patched. • The Organization is reviewing all of its data security practices to identify additional safeguards. • Informed credit reporting agencies and payment card networks about the incident.
<p>Steps taken to notify individuals of the incident</p>	<p>Canadian users who made purchases during the relevant time period were emailed notices of the incident on April 27, 2016.</p>
<p>REAL RISK OF SIGNIFICANT HARM ANALYSIS</p>	
<p>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.</p>	<p>The Organization reported that “It is possible to use the intercepted credit card numbers to make fraudulent purchases.” Further, “The harm is unlikely to be significant. LuckyPet has received no reports of fraudulent purchase from its customers or the credit card companies. Fraudulent purchases that do occur are generally covered by the credit card companies, resulting in no harm to the consumer.”</p> <p>I agree that the financial information at issue could be used to cause the harms of fraud or financial loss. In addition, the email addresses could be used for phishing purposes. These are significant harms.</p>
<p>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.</p>	<p>The Organization reported that “...harm is unlikely, as there have been no reports of fraudulent purchases thus far, and any such purchases are typically covered by the credit card companies.”</p> <p>In my view, the likelihood of harm resulting from this incident is increased because the personal information was accessed with malicious intent by unauthorized parties, and was exposed for approximately 5 months before the Organization became aware of the malicious code.</p>

	<p>The Organization can only speculate that any fraudulent purchases will be “covered by the credit card companies”, even if such transactions are detected.</p>
--	--

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 to cause the significant harms of fraud or financial loss. In addition, the email addresses could be used for phishing purposes. The likelihood of harm resulting from this incident is increased because the personal information was accessed with malicious intent by unauthorized parties, and was exposed for approximately 5 months. The Organization can only speculate that any fraudulent purchases will be “covered by the credit card companies,” even if such transactions are detected.

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 on April 27, 2016 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner