



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Two Leaves and a Bud Tea Company (Organization)
Decision number (file number)	P2016-ND-68 (File #004530)
Date notice received by OIPC	December 15, 2016
Date Organization last provided information	December 15, 2016
Date of decision	December 23, 2016
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 <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)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	<p>The incident involved the following information:</p> <ul style="list-style-type: none">• name,• address,• telephone number,• payment card number, expiry date but NOT security code (CVV). <p>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 e-commerce website.</p>
DESCRIPTION OF INCIDENT	
<input type="checkbox"/> loss <input checked="" type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	
Description of incident	<ul style="list-style-type: none">• On November 29, 2016, the Organization discovered that an unauthorized individual may have accessed the administrative side of its ecommerce website used to process orders.• The Organization investigated and found that information from some orders placed on November 28 and 29, 2016, may have been accessed.

Affected individuals	Affected individuals include one (1) resident of Alberta.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> • Immediately began an investigation. • Remediated the ecommerce website and in the process of strengthening security of website. • Removed stored credit card number from site. • Recommended affected individuals remain vigilant to the possibility of fraud by reviewing their account statements and credit reports for unauthorized activity. • Established a dedicated call centre to respond to any questions.
Steps taken to notify individuals of the incident	The Organization reported it would be notifying the affected individual by letter.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
<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>In assessing the harm that might result from this incident, the Organization reported that “The order information affected here includes payment card information which is generally used to make fraudulent purchases elsewhere online. However, generally card network regulations provide that cardholders are not responsible for fraudulent charges that are timely reported to the issuer of the card.”</p> <p>I agree that the personal information involved could be used to make fraudulent charges, as well as generally cause the harms of identity theft and fraud. These are significant harms that could result to the affected individual as a result of this incident.</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 “Given that in Canada there is zero liability for fraudulent credit card purchases made on an individual’s credit card, there is no risk of significant harm to the affected individual in Alberta arising from this incident. The affected individual will be made whole by their credit card issuer.”</p> <p>In my view, the likelihood of harm resulting from this incident is increased because the breach resulted from malicious intent (deliberate intrusion). The Organization can only speculate that the affected individual “will be made whole by their credit card issuer.” Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud.</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 individual.

The personal information involved could be used to make fraudulent charges, as well as generally cause the significant harms of identity theft and fraud. The likelihood of harm resulting from this incident is increased because the breach resulted from malicious intent (deliberate intrusion). The Organization can only speculate that the affected individual “will be made whole by their credit card issuer.” 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 accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation) and provide me with written confirmation that it has done so on or before January 13, 2017.

Jill Clayton
Information and Privacy Commissioner