



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	ABC Carpet and Home (Organization)
Decision number (file number)	P2017-ND-159 (File #007096)
Date notice received by OIPC	November 9, 2017
Date Organization last provided information	November 9, 2017
Date of decision	November 30, 2017
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify the affected individual in Alberta 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 may have involved the following information:</p> <ul style="list-style-type: none">• name,• address,• telephone number,• email address,• credit card or debit card number, expiration date and security code. <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA. The information was collected through the Organization’s online store.</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 August 9, 2017, the Organization was notified that its online store, which is hosted and maintained by a vendor, may have been compromised.

	<ul style="list-style-type: none"> • The Organization immediately hired an independent computer forensics firm to assist with investigating the incident. • On September 8, 2017, the forensic investigator determined that transaction information for purchases made from January 2, 2017 until August 9, 2017 may have been obtained by unauthorized individuals.
Affected individuals	The incident affected one (1) resident of Alberta.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> • Retained an independent computer forensics firm to assist with the investigation. • Reviewed policies and procedures to ensure vendors are taking appropriate measures to protect information in their control.
Steps taken to notify individuals of the incident	A letter notifying the affected individual in Alberta was mailed on October 9, 2017.
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>The Organization did not specifically identify any harm that might result from this incident, but its notification to affected individuals stated “We recommend you remain vigilant and monitor your credit or debit card statements, and immediately notify your financial institution if you notice any suspicious activity. You should change your password for this account, and any other account if you use the same password, if your log-in credentials were affected by this incident.”</p> <p>In my view, the contact and financial information at issue could be used to cause the harms of identity theft and fraud. In addition, email address could be used to cause the harm of phishing. 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 did not specifically assess the likelihood of harm resulting from this incident but, as noted above, its notification to affected individuals stated “We recommend you remain vigilant and monitor your credit or debit card statements, and immediately notify your financial institution if you notice any suspicious activity. You should change your password for this account, and any other account if you use the same password, if your log-in credentials were affected by this incident.”</p> <p>In my view, the likelihood of harm is increased because the incident was the result of malicious intent (information may have been available to unauthorized individuals) and the personal information was exposed for approximately 7 months.</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 contact and financial information at issue could be used to cause the harms of identity theft and fraud. In addition, email address could be used to cause the harm of phishing. These are significant harms. The likelihood of harm is increased because the incident was the result of malicious intent (information may have been available to unauthorized individuals) and the personal information was exposed for approximately 7 months.

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

I understand the Organization notified the affected individual by letter sent on October 9, 2017. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner