



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Hairbow Center, LLC (Organization)
Decision number (file number)	P2019-ND-002 (File #010466)
Date notice received by OIPC	November 7, 2018
Date Organization last provided information	November 7, 2018
Date of decision	January 2, 2019
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. Pursuant to section 37.1 of the <i>Personal Information Protection Act</i> (PIPA), the Organization is required to notify the individual whose personal information was collected in Alberta.
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”	The incident involved all or some of the following information: <ul style="list-style-type: none">• name,• payment card number, 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. To the extent this personal information was collected in Alberta, PIPA applies.</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 September 26, 2018, the Organization was informed by Shopper Approved, LLC (a third party vendor that provides rating and review services) that a malicious actor modified computer code maintained by Shopper and linked to an image of the Shopper seal which the Organization displayed on its website.

	<ul style="list-style-type: none"> The modified computer code was designed to capture payment card information entered on the Organization’s website and was active from 12:35 a.m. EDT on September 15, 2018 to 11:00 a.m. EOT on September 17, 2018.
Affected individuals	The incident affected 2 Canadian residents, of whom one (1) is a resident of Alberta.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> Immediately removed the Shopper seal from its website. Removed the modified computer code and launched an investigation. Engaged a leading cybersecurity investigation firm to assist with the investigation and began taking steps to enhance security. Contacted law enforcement and will cooperate with any investigation of this incident.
Steps taken to notify individuals of the incident	The Organization reported that notification letters were mailed via first class U.S. mail the week of October 26, 2018.
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 specifically identify any potential harms that might result from this incident but its notification to affected individuals recommended that “you review your current and past credit and debit card account statements for discrepancies or unusual activity. If you see anything that you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued the credit or debit card immediately.” In my view, a reasonable person would consider that the financial information at issue could be used to cause the significant harms of identity theft and fraud.
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 specifically assess the likelihood of harm resulting from this incident. In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because the incident resulted from malicious intent (deliberate action by an unauthorized party). It appears the information was exposed for almost three days.
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.	

A reasonable person would consider that the financial information at issue could be used to cause the significant harms of identity theft and fraud. The likelihood of harm is increased because the incident resulted from malicious intent (deliberate action by an unauthorized party). It appears the information was exposed for almost three days.

I require the Organization to notify the affected individual whose information was collected in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand that notification letters were mailed to affected individuals the week of October 26, 2018. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner