



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	National Baseball Hall of Fame and Museum (Organization)
Decision number (file number)	P2020-ND-021 (File #013659)
Date notice received by OIPC	August 15, 2019
Date Organization last provided information	August 15, 2019
Date of decision	February 14, 2020
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 individuals whose personal information was collected 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 involved the following information:</p> <ul style="list-style-type: none">• name,• address, and• credit or debit card information (including CVV code and expiry date). <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 website, shop.baseballhall.org.</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">• An unauthorized third party injected malicious code into the Organization’s web store.• The code was removed as soon as it was discovered but could have been able to collect information that customers entered on the web store’s check-out page while it was active.

	<ul style="list-style-type: none"> Purchases made via the web store between November 15, 2018 and May 14, 2019 may be affected.
Affected individuals	The incident affected 12 individuals in Alberta.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> Removed the malicious code. Instituted additional security controls and procedures to prevent this type of incident from happening in the future.
Steps taken to notify individuals of the incident	The affected individuals were notified by letter on August 14, 2019.
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 reported possible harms that might result from the breach include “Potential identity theft or financial fraud”.</p> <p>In my view, a reasonable person would consider that the contact and financial information at issue could be used to cause the significant harms of identity theft and fraud.</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 in this case, but reported “Although [the Organization] is not aware of any cases of fraud at this time, the [Organization] notified the affected individuals of this incident and provided the affected individuals with additional guidance on steps they can take to protect themselves moving forward”.</p> <p>In my view, the likelihood of harm resulting from this incident is increased because the incident resulted from malicious intent (deliberate action) and compromised personal information over the course of approximately 6 months.</p>
DECISION UNDER SECTION 37.1(1) OF PIPA	
<p>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.</p> <p>A reasonable person would consider that the contact and financial information at issue could be used to cause the significant harms of identity theft and fraud. The likelihood of harm resulting from this incident is increased because the incident resulted from malicious intent (deliberate action) and compromised personal information over the course of approximately 6 months.</p>	

I require the Organization to notify the affected individuals whose personal information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand affected individuals were notified by letter on August 14, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner