Office of the Information and Privacy Commissioner of Alberta

PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Big Idea Entertainment, LLC (Organization)
Decision number (file number)	P2016-ND-57 (File #000866)
Date notice received by OIPC	May 14, 2015
Date Organization last provided information	August 24, 2015
Date of decision	August 31, 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 *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is a Tennessee-based company that is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • address, • email address, • telephone number, • credit card number, expiry date and security code (CVV). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected via the Organization's Veggietales.com website which includes an online shopping service.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• The Organization owns and operates the Veggietales.com website. The website includes an online shopping service. • The website uses third party software to support its online shopping service. The Organization was advised by its third party software provider that a vulnerability in the software had been identified. • The Organization patched the vulnerability and conducted an investigation to see whether the vulnerability had been exploited prior to the patching. • The investigation revealed that an unauthorized and unknown third party compromised the website between April 24 and 29, 2015 and had accessed the personal information of some website visitors.
Affected individuals	A total of 73 individuals were affected, including one Alberta resident.
Steps taken to reduce risk of harm to individuals	• Investigated to determine whether the vulnerability had been exploited. • Patched the vulnerability and implementing a new process to ensure that higher risk vulnerabilities are patched promptly upon notification. • Conducted an internal investigation to identify all affected individuals and the personal information that was impacted.
Steps taken to notify individuals of the incident	The affected individual in Alberta was notified by letter on May 8, 2015.
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 reported that "Aside from the credit card data, the personal information involved in this incident is generally considered non-sensitive (name, address, email address). Credit card data may be used to perpetrate fraud and the breach format indicates that this was the intent of the unauthorized third party." The Organization also reported that "… email addresses may sometimes be used successfully in phishing schemes." I agree with the Organization that the financial information involved in this incident could be used to cause the harms of identity theft, fraud and financial loss. Email addresses could be used for phishing purposes. These are significant harms.

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 reported "… 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 the compromise of their credit card information. The affected individual will be kept whole by their credit card issuer. There may be some inconvenience associated with a replacement credit card, but that is not a significant harm." With respect to the possible phishing risk, the Organization reported "…the very low number of affected individuals, overall, and the nature of the Veggietales.com website store (i.e. a store that sells goods designed for children), makes this use improbable and the fact that the unauthorized third party specifically sought out credit card information strongly indicates that credit card fraud was the ultimate goal of the intrusion." In my view, there is a real risk of harm resulting from this incident. The likelihood is increased because the personal information was accessed in an unauthorized manner with malicious intent, and was exposed for 5 days. The circumstances of the incident suggest the information at issue was the target, and, while it may be that the perpetrators sought out credit card information, this cannot be known for sure; phishing is also a real possibility. The nature of the website (selling goods designed for children) does not seem to me to be a factor that reduces the likelihood of risk, given that the contact and financial information at issue is that of adults who would likely be the potential targets of credit card fraud or phishing. The Organization can only speculate that affected individuals will not be held responsible for fraudulent credit card purchases, and does not have any control over this remedy. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud, or the already noted possible use of the information for phishing purposes.
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 involved in this incident could be used to cause the harms of identity theft, fraud and financial loss. Email addresses could be used for phishing purposes. These are significant harms.	

The circumstances suggest the information at issue was the target, and, while it may be that the perpetrators sought out credit card information, this cannot be known for sure; phishing is also a real possibility. The nature of the website (selling goods designed for children) does not seem to me to be a factor that reduces the likelihood of risk, given that the contact and financial information at issue is that of adults who would likely be the potential targets of credit card fraud or phishing. The Organization can only speculate that affected individuals will not be held responsible for fraudulent credit card purchases, and does not have any control over this remedy. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud, or the already noted possible use of the information for phishing purposes.

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

I understand the Organization notified the affected individuals, including the resident of Alberta, by letter dated May 8, 2015, in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner