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	Nite Ize, Inc. (Organization)
Decision number (file number)	P2016-ND-48 (File #000563)
Date notice received by OIPC	March 27, 2015
Date Organization last provided information	March 27, 2015
Date of decision	August 23, 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 incorporated in Boulder, Colorado, United States and 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, • user name, • password, • credit card number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected from residents of Alberta.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization operates a consumer-facing website, which is hosted and managed by a third party website service provider. • On March 11, 2015, the Organization learned from its service provider that it had experienced a cyber-attack and credit card information was compromised for orders processed between March 3 and March 11, 2015. • The Organization took immediate steps to remove the malicious code that the hackers had inserted. • The Organization's service provider has been unable to determine whether the general customer database was actually accessed, but could not rule out the possibility.
Affected individuals	The incident affected 383 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Retained a cybersecurity forensics investigator to investigate and remove the malicious code. • Required all users of the website to reset their passwords the next time they logged in. • Alerted affected individuals' bank and credit card companies.
Steps taken to notify individuals of the incident	Affected individuals were notified by email March 30, 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 the affected individuals' personal information could be used for fraud, and also noted that "if the customer used the same password for other online services or accounts, then such other services or online accounts could be subject to unauthorized access." I agree with the Organization. The information at issue could be used to cause the harms of identity theft, fraud and financial loss. Passwords, if accessed, could be used to compromise other online accounts, and email addresses and other information 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 that "Because our website service provider has data that indicates the affected credit cards could have been compromised, there is a likelihood that the credit card numbers could be used for fraudulent activities…. Because our service provider has been unable to determine whether the generic customer database was actually accessed, predicting the likelihood of any resulting harm is difficult." In my view, the likelihood of harm resulting from this incident is increased because the incident was the result of a deliberate intrusion by an unauthorized party. Despite the fact the Organization was unable to confirm whether certain information had been accessed, it could not rule this possibility out, which in my view, increases the risk of harm.

DECISION UNDER SECTION 37.1(1) OF PIPA

Based on the information provided by the Organization and given the circumstances of this incident, I have decided that there is a real risk of significant harm to the affected individuals.

The information at issue could be used to cause the harms of identity theft, fraud and financial loss. Passwords, if accessed, could be used to compromise other online accounts, and email addresses and other information could be used for phishing purposes. These are significant harms. The likelihood of harm resulting from this incident is increased because the incident was the result of a deliberate intrusion by an unauthorized party. Despite the fact the Organization was unable to confirm whether certain information had been accessed, it could not rule this possibility out, which in my view, increases the risk of harm.

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

I understand the Organization notified the affected individuals by email on March 30, 2015. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner