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	Kathmandu (U.K) Limited, Kathmandu Limited, and Kathmandu Pty Limited (Organization)
Decision number (file number)	P2019-ND-134 (File #012892)
Date notice received by OIPC	March 28, 2019
Date Organization last provided information	March 28, 2019
Date of decision	August 13, 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 *Personal Information Protection Act* (PIPA), the Organization is required to notify those individuals 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 the following information: • name, • address, • credit card information, and • username and password, if provided. 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.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On or about February 21, 2019, the Organization became aware that an unidentified third party gained unauthorized access to its website between January 8, 2019 and February 12, 2019. During this process, the third party may have captured customer personal information and payment details entered at check-out for potential fraudulent use.

Affected individuals	The incident affected 3 individuals in Alberta
Steps taken to reduce risk of harm to individuals	• Confirmed that the online store and wider IT environment were secure. • Working with external IT and Cyber Security consultants to fully investigate the circumstances of the incident. • Providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank.
Steps taken to notify individuals of the incident	Affected individuals were notified on or about March 13, 2019.
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 harm(s) that might result from this incident, but did report that it "…is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank." In my view, a reasonable person would consider the contact and financial information at issue could be used to cause the significant harms of identity theft and fraud. Credentials could be used to compromise other online accounts. 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 did not assess the likelihood of harm resulting from this breach. In my view, a reasonable person would consider the likelihood of harm resulting in this case is increased because the incident appears to be the result of deliberate, malicious action. The information was exposed for over a month.
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 the contact and financial information at issue could be used to cause the significant harms of identity theft and fraud. Credentials could be used to compromise other online accounts. These are significant harms. The likelihood of harm resulting in this case is increased because the incident appears to be the result of deliberate, malicious action. The information was exposed for over a month.	

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 the Organization notified the affected individuals on or about March 13, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner