Kathmandu®

<<Date>> (Format: Month Day, Year)

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

RE: Notice of Data Breach

Dear <<FirstName>> <<LastName>>,

We are writing to let you know of a recent security incident with our website. This incident may have affected customers who made purchases from a Kathmandu website between January 8, 2019 NZDT and February 12, 2019 NZDT*. The systems used by our physical stores have not been impacted by this incident.

This notification explains what happened, how it may impact you and steps you can take in response.

What Happened?

We have recently become aware that between January 8, 2019 and February 12, 2019, an unidentified third party gained unauthorized access to our website. During this process, the third party may have captured customer personal information and payment details entered at check-out for potential fraudulent use.

As soon as we became aware of this incident, we took immediate steps to confirm that our online store and our wider IT environment was secure. Since this time, we have been working closely with leading external IT and Cyber Security consultants to fully investigate the circumstances of the incident and confirm which customers may have been impacted.

Our number one focus has been to clearly identify who has been (and rule out who has not been) potentially affected by this incident and also identify precisely what information is involved so we can meaningfully inform you about how you may have been affected.

What Information Was Involved?

The personal information which could have been impacted by the incident may include some or all of the following categories of information (if provided by you):

- billing and shipping name, address, email and phone number;
- the credit/debit card details you provided to complete the purchase; and
- your Kathmandu Summit Club login username and password.

We believe that no other information about you was impacted by this incident. For those customers who made purchases using Afterpay or PayPal, there is no evidence to suggest that your Afterpay or PayPal login details and information collected by these platforms (including financial) has been impacted.

What We Are Doing:

As an organization, we take the protection of personal information within our care very seriously. Upon learning of this incident, we quickly took steps to prevent further unauthorized access to our systems. We have been and will continue to work with the relevant authorities and security experts. We are providing notice to all relevant US authorities.

What You Can do:

If you used a credit or debit card on our site between January 8, 2019 and February 12, 2019, we recommend that you review and continue to monitor your financial and payment card account statements for any discrepancies or unusual activity. Contact your financial institution if you have any concerns.

Because your contact information may also be affected, we recommend that you:

- change all passwords that may have been identical or similar to the password used to access the Kathmandu online account service (such as email, social media, online banking etc); and
- remain vigilant around email, telephone and text-based scams.

As a precautionary step, if you did not reset your Kathmandu Summit Club password after 12 February 2019, we have reset it for you.

Please review the "Steps You Can Take to Protect Your Information" to learn more about ways to protect personal information.

For More Information:

We are deeply sorry for any disruption that this incident causes for our customers. We can assure you that we are doing everything we can to ensure the ongoing security of our systems to help prevent this type of incident occurring again in the future.

You can contact our information line by calling **1-866-775-4209**, Monday through Friday from 8:00am to 5:30pm Central Time for more information and support.

We have also set up a dedicated webpage www.kathmanduoutdoor.com/security-incident which contains answers to FAQS, advice about the steps you can take to protect your information and a dedicated email mailbox privacy@kathmandu.com.au should you have any further questions.

Kind regards

Kathmandu

** Due to time zone differences the date range may include 7 January 2019 (GMT) and end on 11 February 2019 (GMT).*

Steps You Can Take to Protect Your Information

Monitor Your Accounts.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-909-8872
www.transunion.com/credit-freeze

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19106
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us. Kathmandu Limited is located at 223 Tuam Street, Christchurch Central, Christchurch, 8011, New Zealand.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.