LEWIS BRISBOIS BISGAARD & SMITH LLP

Sean B. Hoar
888 SW Fifth Avenue, Suite 900
Portland, Oregon 97204-2025
Sean.Hoar@lewisbrisbois.com
Direct: 971.712.2795

August 1, 2018

VIA ELECTRONIC SUBMISSION

Attorney General Bob Ferguson
Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
E-Mail: SecurityBreach@atg.wa.gov

Re: Notification of Data Security Incident - Update

Dear Attorney General Ferguson:

We represent Manduka in connection with the recent data security incident described in greater detail below about which we notified you on March 27, 2018 and on June 8, 2018.

1. Nature of the security incident.

On February 25, 2018, Manduka learned of a potential data security incident involving the unauthorized installation of malware on its e-commerce web platform. Upon discovering this incident, Manduka took steps to secure customer payment card information and contacted law enforcement. In addition, Manduka launched an investigation and engaged a leading forensics firm to determine what happened and whether customer payment card information had been accessed or acquired without authorization. It appears that payment card information including names, card numbers, expiration dates, and security codes belonging to customers who utilized the Manduka web platform from February 22, 2017 to March 5, 2018 was affected.

On May 20, 2018, Manduka learned that payment card information belonging to customers who utilized the Manduka web platform from May 18, 2018 to May 20, 2018 could have been affected as well as a result of the unauthorized reinstallation of malware on its e-commerce web platform. Manduka's ongoing monitoring efforts resulted in the identification and removal of this malware within two days of its reinstallation.

On July 6, 2018, Manduka learned that payment card information belonging to customers who utilized the Manduka web platform from July 5, 2018 at approximately 11:00 A.M. Pacific Time to July 6, 2018 at approximately 2:00 P.M. Pacific Time could have been affected as well as a result of the unauthorized reinstallation of malware on its e-commerce web platform. Manduka's ongoing monitoring efforts resulted in the identification and removal of this malware within one day of its reinstallation. Manduka is now in the process of taking additional steps to enhance its security.

2. Number of Washington residents affected.

Manduka notified 1,634 Washington residents of this incident on March 26, 2018 and notified an additional 7 Washington residents of this incident on June 8, 2018. Finally, Manduka notified 7 Washington residents of this incident on August 1, 2018. A copy of the notification letter provided to individuals impacted between July 5, 2018 and July 6, 2018 is enclosed.

3. Steps taken relating to the incident.

Manduka has taken affirmative steps to prevent a similar situation from arising in the future and to protect the privacy and security of all sensitive information. These steps have included working with a leading forensics firm to remove malicious code from its e-commerce web platform, to block traffic to / from malicious domains, and to continuously monitor the Manduka system. Manduka has also taken numerous steps to secure its e-commerce platform (Magento), including but not limited to implementing multi-factor authentication for Magento access. In addition, Manduka is working to transition from Magento to use of a cloud-based e-commerce platform and is in the process of rebuilding its e-commerce website from scratch in order to bolster security.

4. Contact information.

Manduka is committed to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at (971) 712-2795, or by e-mail at Sean.Hoar@LewisBrisbois.com.

Sincerely,

Sean B. Hoar of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure

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

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Subject: Notice of Data Breach

Dear <<MemberFirstName>> <<MemberLastName>>,

I am writing to inform you of a data security incident that may have affected your payment card information. At Manduka, we take the privacy and security of your information very seriously and regret any concern that this incident may cause you. That is why we are contacting you and informing you about steps that can be taken to protect your information.

What Happened? On July 6, 2018, Manduka learned of a potential data security incident involving the unauthorized installation of malware on our e-commerce web platform. Upon discovering the incident, we took immediate steps to secure this information. We also launched an investigation and worked with a leading forensics firm to determine what happened and whether customer payment card information had been accessed or acquired without authorization. This letter serves to inform you of the incident and to share with you steps that you can take to help protect your information.

What Information Was Involved? We believe that the malware could have comprised payment card information belonging to customers who utilized our web platform to purchase products from July 5, 2018 to July 6, 2018. The affected payment card information may have included names, card numbers, expiration dates, and security codes.

What Are We Doing? As soon as Manduka discovered the incident, we took the steps described above. We also reported the incident to the Federal Bureau of Investigation ("FBI") and are working with both the FBI and the United States Secret Service to hold the perpetrators accountable. In addition, we reported the matter to the payment card brands to protect your payment card information and prevent fraudulent activity. We are also providing you with information about steps that you can take to help protect your personal information. Finally, we take the security of all personal information very seriously and have taken steps to enhance the security of Manduka customer information and our e-commerce web platform in order to prevent similar incidents from occurring in the future.

What You Can Do: You can follow the recommendations on the following page to protect your personal information. We recommend that you review your current and past credit and debit card account statements for discrepancies or unusual activity. If you see anything that you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued the credit or debit card immediately.

For More Information: Further information about how to protect your personal information appears on the following page. If you have questions please call 1-???-???-???? (toll free), Monday through Friday from 8:00 a.m. to 5:00 p.m. Central Time, excluding major holidays.

Thank you for your loyalty to Manduka and your patience through this incident. We take your trust in us and this matter very seriously. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Beau Swenson

Beau J. Swenson
Chief Financial Officer

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can also contact one of the following three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**	**Free Annual Report**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-800-525-6285	1-888-397-3742	1-877-322-8228	1-877-322-8228
www.equifax.com	www.experian.com	www.transunion.com	www.annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: In some U.S. states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. If you request a security freeze from a consumer reporting agency there may be a fee up to $10 to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
401-274-4400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.