August 31, 2018

VIA OVERNIGHT MAIL AND EMAIL

The Honorable Joseph Foster
Consumer Protection and Antitrust Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
DOJ-CPB@doj.nh.gov

RE: Bombas, LLC

Dear Attorney General Foster:

On behalf of Bombas, LLC ("Bombas"), I am writing to update you regarding a matter involving unauthorized access to personal information for which we have provided notice on May 18, 2018.

In the May 2018 Notice, we reported that, among other things, Bombas experienced a security incident on its website ("Website") due to malicious code in the Magento code of its third party e-commerce platform used for payment card purchases. We further reported that the malicious code was initially identified and removed from the Website on January 15, 2015 and then finally removed on February 9, 2015; that there was no definitive way for Bombas to identify which transactions were impacted. As a result, Bombas provided notice[1] to all approximately 41,000 customers who made a payment card purchase on the Website during the period that Bombas believed malicious code may have existed. At that time, we set the exposure date from the launch of the Website (set at the time as September 1, 2013), until the day the identified malicious code was finally disabled (February 9, 2015).[2]

During its ongoing further review, Bombas uncovered a copy of the code for the Website at the relevant time, including the malicious code, and other evidence supporting the conclusion that the unauthorized access to personal information (i.e., customer names, addresses, and credit card

[1] The May 2018 Notice also explained that, during the time after its discovery, Bombas disclosed the matter to the payment card brands, which did not require a formal PFI or otherwise pursue the matter beyond basic questions, leaving Bombas management to conclude that the incident was resolved. However, Bombas revisited the matter in the course of a 2018 review and thereafter provided notice to customers and regulators.

[2] As also explained in the May 2018 Notice, notices were not being provided to customers who purchased by (i) credit card from January 15, 2015 to January 27, 2015, as the malicious code was disabled during such period (only to reappear from January 27, 2015 to February 9, 2015); and (ii) PayPal, as its method of payment card entry was not affected by the vulnerability.

information) most likely did not begin until September 27, 2014, at the earliest, and that the malicious code was not present at the time of Website launch in September 2013. In short, the initial definition of the exposure period overstated the exposure by at least 12 months. In addition, Bombas discovered that, although the malicious code was disabled on February 9, 2015 (likely ending potential exposure to the malicious code), remediation activities continued through February 25, 2015. As such, Bombas is now extending the end date by 16 days for the window of exposure from February 9, 2015 to February 25, 2015.

Based on this updated potential exposure window, the total number of potentially affected individuals is approximately 39,561, approximately 252 of whom appear to be New Hampshire residents.[3] Further, of those 252 residents, approximately 12 appear to be within the universe of individuals who made purchases only between February 10, 2015 and February 25, 2015 and therefore would not have received a notice in May 2018. This week, Bombas will send a letter to each of these 12 individuals for whom the window of exposure is February 10, 2015 to February 25, 2015, notifying and informing them of the matter. The form of the notification letter to be sent to the affected persons in New Hampshire is enclosed.

Bombas is offering all customers who are receiving notice credit monitoring and identity theft protection services through Kroll Information Assurance, LLC for a twenty-four (24) month period.

Since February 2015, Bombas has put a number of measures in place to enhance website security, and also now runs on an entirely different e-commerce platform. Consistent with Bombas' commitment to privacy and security, we have more recently conducted a privacy and data security program review, which has resulted in the development or enhancement of policies and training on reasonable and appropriate security measures designed to protect personal information, including by third party vendors and on managing data incidents.

If you should have any additional questions or need further information regarding this incident, please do not hesitate to contact me at 646-760-8112.

Sincerely,

David Heath
Co-Founder and Chief Executive Officer

Enclosure

[3] Similar to the May 2018 notices, supplemental notices are not being provided to customers who made a purchase using PayPal, as its method of payment card entry was not affected by the vulnerability.

BOMBAS

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

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

NOTICE OF DATA BREACH

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

The two things we take most seriously at Bombas are our efforts to improve the community where we all work and live and your security and satisfaction as a Bombas customer and supporter. That's why we're writing you today.

In our commitment to your privacy and security, we are conducting a thorough review of our data security safeguards and data breach response policies and procedures. In connection with this review, we are sending this notice to let you know about a historical data security incident.

What Happened?

We first started selling Bombas socks online through our website in September 2013. We relied on larger, professional third party service providers for the design, development, hosting, maintenance, backend credit card processing, and security of our website.

Previously, Bombas provided notice to affected customers in relation to a historical cybersecurity incident involving an unknown attacker who injected malicious code into our website in late 2014, which we identified and fixed in early 2015 (the "Incident"). At the time of the prior notice, Bombas believed that malicious code was disabled fully on February 9, 2015.

Earlier this month, however, Bombas re-examined the issue and concluded that there was some chance of potential exposure until February 25, 2015. In light of this discovery, Bombas is now sending this notice to all those customers who made purchases between February 10, 2015 and February 25, 2015, just in case they were affected by the Incident.

What Information was Involved?

The data accessed may have included personal information such as name, address, and credit card information. On the Bombas website, we never request any Social Security numbers or other identification numbers, and these identification numbers could not have been impacted.

What Are We Doing?

We value you as a Bombas customer and supporter and are extremely sorry that this Incident occurred in the first place. Out of an abundance of caution, we are offering you free identity monitoring for two years.

Since the Incident, we have implemented additional security measures designed to prevent a recurrence of such an attack and to protect the privacy of all Bombas customers. Today, we run on an entirely different e-commerce platform.

To assist in supporting and protecting our customers, we have engaged a trusted third-party service provider, Kroll, to provide you with more information as outlined below.

What Can You Do?

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

We advise you to remain vigilant by reviewing your account statements and monitoring your credit reports regularly. If you see unauthorized activity on your account statements, you should contact your financial institution or payment card issuer directly. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities and/or the Federal Trade Commission (FTC).

Enroll in the Free Identity Monitoring Services

In addition, we have arranged with Kroll to provide you with identity monitoring services to include credit monitoring and fraud consultation and identity theft restoration for two years, at no cost to you. Kroll is a global leader in risk mitigation and response and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services are further described on the enrollment website. Visit **my.idmonitoringservice.com** to enroll and take advantage of your identity monitoring services. **You have until November 29, 2018 to activate your identity monitoring services.**

Membership Number **<<Member ID>>**

For More Information

For further information and assistance, please contact Kroll toll free at 1-800-319-4823 between 9am – 6pm Eastern Time. We have set up this hotline so that we can personally address any concerns you might have in light of this notice. Please also review the attached additional information for helpful steps you can take to protect your identity.

Please let us restate that we take very seriously our responsibility to safeguard your personal information. We sincerely apologize for the worry this situation may cause you.

Again, please accept our apologies.

Sincerely,

David Heath
Co-Founder and Chief Executive Officer

Kroll

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Important Identity Theft Information: Additional Steps You Can Take to Protect Your Identity

The following are additional steps you may wish to take to protect your identity.

Review Your Accounts and Credit Reports

Regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. When you receive your credit report, look it over with care. If you notice anything suspicious – accounts you did not open, inquiries from creditors that you did not initiate, personal information such as a home address or Social Security number that is not accurate – or you see anything you do not understand, call the credit reporting agency at the number listed in the report. If you find fraudulent or suspicious activity in your credit reports, you should promptly report the matter to the proper law enforcement authorities. Follow the steps recommended above for reporting fraudulent or suspicious activity to law enforcement.

You may obtain a free copy of your credit report online at www.annualcreditreport.com by calling toll free 1.877.322.8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service. P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax Credit Information Services, Inc.
P.O. Box 740241
Atlanta, GA 30374
(888) 685-1111
www.equifax.corn

Experian
P.O. Box 4500
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion
2 Baldwin Place
P.O. Box 1000
Chester, PA 19016
(800) 888-4213
www.transunion.com

Consider Placing a Fraud Alert

You may wish to consider contacting the fraud department of the three major credit bureaus to request that a "fraud alert" be placed on your file. A fraud alert notifies potential lenders to verify your identification before extending credit in your name.

Equifax:	Report Fraud:	1.888.766.0008
Experian:	Report Fraud:	1.888.397.3742
TransUnion:	Report Fraud:	1.800.916.8800

Security Freeze for Credit Reporting Agencies

You may wish to request a security freeze on your credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $10.00, (or in certain states such as Massachusetts, no more than $5.00), each to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the following addresses:

- Equifax Security Freeze, P.O. Box 105788, Atlanta, GA 30348
- Experian Security Freeze, P.O. Box 9554, Allen, TX 75013
- TransUnion Security Freeze, Fraud Victim Assistance Department, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016

To request a security freeze, you will need to provide the following:

- Your full name (including middle initial, Jr., Sr., Roman numerals, etc.)
- Social Security number
- Date of birth
- Address(es) where you have lived over the prior five years
- Proof of current address such as a current utility bill
- A photocopy of a government-issued ID card
- If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.
- If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Don't send cash through the mail.

The credit reporting agencies have three business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include (1) proper identification (name, address, and Social Security number), (2) the PIN number or password provided to you when you placed the security freeze; and (3) the

identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze all together, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three business days after receiving your request to remove the security freeze.

You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

Suggestions If You Are a Victim of Identity Theft

- File a police report. Get a copy of the report to submit to your creditors and others that may require proof of a crime.
- Contact the U.S. Federal Trade Commission (FTC). The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by calling the FTC's Identity Theft Hotline: 1.877.IDTHEFT (1.877.438.4338); online at http://www.ftc.gov/idtheft; or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580. Also request a copy of the publication, "Take Charge: Fighting Back Against Identity Theft" from: http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.pdf.
- Keep a record of your contacts. Start a file with copies of your credit reports, the police reports, any correspondence, and copies of disputed bills. It is also helpful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

Take Steps to Avoid Identity Theft

Further information can be obtained from the FTC about steps to take to avoid identity theft through the following paths: http://www.ftc.gov/idtheft; calling 1.877.IDTHEFT (1.877.438.4338); or write to Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580.

State-Specific Information

Iowa residents may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached by visiting the website at www.iowaattorneygeneral.gov, calling (515) 281-5164 or requesting more information from the Office of the Attorney General, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

Maryland residents can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting their web site at http://www.oag.state.md.us/idtheft/index.htm, calling the Identity Theft Unit at 1.410.567.6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202.

New Mexico residents are reminded that you have the right to obtain a police report and request a security freeze as described above and you have rights under the Fair Credit Reporting Act as described above.

North Carolina residents can learn more about preventing identity theft from the North Carolina Office of the Attorney General, by visiting their web site at http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx, calling 1.919.716.6400 or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center Raleigh, NC 27699-9001.

Oregon residents may obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached by visiting the website at www.doj.state.or.us, calling (503) 378-4400 or requesting more information from the Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.

Rhode Island residents are reminded that you have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may charge you a small fee to place a security freeze on your account, and may require that you provide certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. There is no charge, however, to place, lift or remove a security freeze if you have been a victim of identity theft and you provide the consumer reporting agencies with a valid police report. Residents can learn more by contacting the Rhode Island Office of the Attorney General by phone at 1.410.274.4400 or by mail at 150 South Main Street, Providence, Rhode Island 02903.

Vermont residents may learn helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report on the Vermont Attorney General's website at http://www.atg.state.vt.us.