ROPES & GRAY LLP
2099 PENNSYLVANIA AVENUE, NW
WASHINGTON, DC 20006-6807
WWW.ROPESGRAY.COM

June 3, 2020

Edward R. McNicholas
T +1 202 508 4779
edward.mcnicholas@ropesgray.com

BY E-MAIL

Attorney General Tom Miller
Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106
consumer@ag.iowa.gov

Re: Data Incident

Dear General Miller:

We write on behalf of our client, Bombas LLC, to inform you of a security incident that may have affected the personal information of approximately 965 Iowa residents.

On December 26, 2018, Bombas received a Common Point of Purchase (CPP) report from BrainTree, which resulted in a rapid review of its security. By January 3, 2019, Ropes & Gray had been retained and engaged Stroz Friedberg, who had located and analyzed malicious code operating in its Shopify e-commerce site. By January 10, 2019, Stroz Friedberg concluded, however, that the malicious code was not functional; and on January 14, 2019, Shopify assured Bombas that its security features "result in the malware being rendered innocuous."

In late 2019, as part of a review of data security, Bombas discovered that the same malicious code designed to scrape credit card numbers and other personal information may have been present as early as November 11, 2016. Bombas promptly re-launched a thorough investigation to determine whether personal information of its customers had been potentially exposed by the code that it had been assured was "innocuous" earlier that year.

On May 20, 2020, after extensive investigative work, Stroz Friedberg issued the report of its investigation ("May 2020 Stroz Report"). Like the January 2019 report, the May 2020 Stroz Report found that the Shopify security features prevented the malicious code from functioning. The May 2020 Stroz Report also found that the Shopify security feature was added to Bombas' e-commerce platform only on February 16, 2017. Accordingly, the May 2020 Stroz Report could

not rule out the possibility that the malicious code could have successfully scraped customer information between November 11, 2016 and February 16, 2017.

The malicious code, when functional, could have enabled the attacker to acquire certain personal information belonging to customers who entered their payment card information in its online checkout process during the relevant period. The affected information may have included customer name, address, and payment card data.

In addition to exhaustively investigating any concerns about the security of its website, Bombas has taken and is taking steps to protect the security of its customers' information including investments in the people, processes, and technologies that drive its comprehensive information security program. Its discovery of this incident is a result of those cybersecurity efforts, and its reporting of this possible exposure of information is an indication of Bombas' cultural commitment to protecting its customers.

Bombas has made arrangements for potentially affected customers to receive two years of credit monitoring at no cost to them. Additional information on credit monitoring services and a telephone number consumers may call for further information and assistance is included in the attached sample notification made to the affected parties. This notice will be mailed to potentially affected customers beginning June 3, 2020.

If you have any questions, please contact us at (202)-508-4779.

Sincerely,

Edward R. McNicholas

BOMBAS

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We recently discovered information regarding a past security incident that may have involved your personal information. We are writing to share with you some important information about this incident.

What Happened?

Last year, as part of a review of data security, we discovered that malicious code designed to scrape credit card numbers and other personal information may have been present as early as November 11, 2016 on our e-commerce platform. We launched a thorough investigation to determine whether personal information of our customers was potentially exposed.

On May 20, 2020, we received an investigative report, which could not rule out the possibility that the malicious code could have successfully scraped customer information. The report also confirmed that a new security feature, which was added to our e-commerce platform on February 16, 2017, prevented the malicious code from functioning after that date. Accordingly, there is a window from November 11, 2016 to February 16, 2017 during which customer information potentially could have been exposed.

What Information Was Involved?

We believe that the malicious code could have enabled the attacker to acquire certain personal information belonging to customers who entered their payment card information in our online checkout process during the relevant period. The affected information may have included your name, address, and payment card data.

What We Are Doing.

We take the security of our customers' information seriously. In February 2017, a feature was added to our e-commerce platform that would prevent malicious code attacks like this one. We have also taken other steps in recent years to further improve security and prevent similar incidents from happening in the future. Our discovery and reporting of this incident is a result of those cybersecurity efforts.

What You Can Do.

In addition to the steps we have taken, you can take action to protect your personal information. Under U.S. law, you are entitled to one free credit report annually from each of the three nationwide credit reporting agencies. To order a free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228.

As always, we encourage you to regularly review your financial accounts and report any suspicious or unrecognized activity immediately. The enclosed "Important Identity Theft Information" provides further information about what you can do. As recommended by federal regulatory agencies, you should remember to be vigilant and report any suspected incidents of fraud to the relevant financial institution.

Other Important Information.

In order to assist you with this vigilance, we have made arrangements to provide you with identity monitoring services at no cost to you for two years, should you wish to participate. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **September 1, 2020** to activate your identity monitoring services.*

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

Additional information describing your services is included with this letter.

We regret this incident and any inconvenience to you. If we can be of help in any way, please contact our dedicated call center at 1-844-994-2101, Monday through Friday, from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

Sincerely,

David Heath
Co-Founder and Chief Executive Officer

Important Identity Theft Information: Additional Steps You Can Take to Help 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. 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,** P.O. Box 740241, Atlanta, Georgia 30374-0241. 1.866.349.5191. www.equifax.com
- **Experian,** P.O. Box 9532, Allen, TX 75013. 1.888.397.3742. www.experian.com
- **TransUnion,** 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016. 1.800.888.4213. 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:	1.800.525.6285
Experian:	Report Fraud:	1.888.397.3742
TransUnion:	Report Fraud:	1.800.680.7289

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. It is free to place, lift or remove a security freeze.

You must separately place a security freeze on your credit report at each credit bureau. To do so, you must contact the credit bureaus by phone, mail, or secure electronic means:

- **Equifax:** P.O. Box 105788, Atlanta, GA 30348, 1.888.298.0045, www.Equifax.com
- **Experian:** P.O. Box 9554, Allen, TX 75013, 1.888.397.3742, www.Experian.com
- **TransUnion:** P.O. Box 2000, Chester, PA 19106, 1.888.909.8872, www.TransUnion.com

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 request a freeze online or by phone, the agency must place the freeze within one business day. The credit bureaus have three business days after receiving a request by mail to place a security freeze on your credit report, and they must also send 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 contact the credit reporting agencies and include (1) proper identification; (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.

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 (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 helpful to log 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 at: http://www.ftc.gov/idtheft; calling 1-877-IDTHEFT (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 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. 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.

Kroll | A Division of DUFF & PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services 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 will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

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 will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
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.