MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

James E. Prendergast
Office: 267-930-4798
Fax: 267-930-4771
Email: jprendergast@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

January 5, 2018

VIA U.S. 1st CLASS MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Attorney General MacDonald:

Our office represents Rea.deeming Beauty, Inc. d/b/a beautyblender ("beautyblender") 3864 Courtney Street, Bethlehem, PA 18017. We are writing to provide you with notice of an event that may impact the security of certain payment information relating to approximately fifty-eight (58) New Hampshire residents. By providing this notice, beautyblender does not waive any rights or defenses regarding the applicability of New Hampshire law, applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Background

Beautyblender was recently contacted by two customers reporting fraud on credit cards used to make purchases on our site. Beautyblender immediately launched an internal investigation and contacted its website hosting company. The website hosting company discovered what it believed was a form of malicious code on beautyblender's site on October 26, 2017 which it then removed. A third party forensic investigator was also retained to assist with beautyblender's investigation. On November 27, 2017, the forensic investigator confirmed that the malware inserted into the website collected certain payment card information used at checkout. The forensic investigator then began efforts to determine when the malware was placed on the website. Unfortunately, due to the lack of backups of the website that were available from the website hosting company, beautyblender has been unable to confirm the date that the malware was placed on the website.

The forensic investigator confirmed that the malware was in place as of July 28, 2017. The next most recent backup available was from April 23, 2015 which did not have evidence of the malware. While

beautyblender and the forensic investigator do not believe the malware was present during this entire time period, beautyblender has no contrary evidence and is notifying all customers who made purchases on its website during this time period in an abundance of caution.

The specific information that may have been obtained by the unidentified third party included the customers' name, billing address, full credit card number, expiration date and CVV number. Beautyblender removed the malicious code from the website, and took additional steps to ensure the security of its systems.

Notice to New Hampshire Residents

On January 5, 2018, beautyblender will begin providing written notice of this incident to all potentially affected customers, which includes fifty-eight (58) New Hampshire residents. Written notice will be provided in substantially the same form as the letter attached hereto as ***Exhibit A***.

Other Steps Taken and To Be Taken

Immediately after discovering the malicious code, beautyblender initiated efforts to remove it from the website. In addition, beautyblender is providing potentially affected individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification of other aspects of this event, please contact us at 267-930-4798.

Very truly yours,

James E. Prendergast of
MULLEN COUGHLIN LLC

JEP:ncl
Enclosure

EXHIBIT A

Rea.deeming Beauty, Inc.
home of
the original beautyblender
Processing Center • P.O. BOX 141578 • Austin, TX 78714

00002
ACD1234

00353
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

January 5, 2018

RE: Notice of Data Breach

Dear John Sample:

Rea.deeming Beauty, Inc. dba beautyblender ("beautyblender") is writing regarding a recent data security incident that may impact certain payment card information used by you to make purchases on our website. We wanted to provide you with information about this incident, our response and steps you can take to prevent fraud, should you feel it necessary to do so.

What Happened? Beautyblender was recently contacted by two customers reporting fraud on credit cards used to make purchases on our site. We immediately launched an internal investigation and contacted our website hosting company. The website hosting company discovered what it believed was a form of malicious code on our site on October 26, 2017 which it then removed. A third party forensic investigator was also retained to assist with our investigation. On November 27, 2017, the forensic investigator confirmed that the malware inserted into our website collected certain payment card information used at checkout. The forensic investigator then began efforts to determine when the malware was placed on our website. Unfortunately, due to the lack of backups of our website that were available from our website hosting company, we have been unable to confirm the date that the malware was placed on our website.

The forensic investigator confirmed that the malware was in place as of July 28, 2017. The next most recent backup available was from April 23, 2015 which did not have evidence of the malware. While we do not believe the malware was present during this full time period, we have no contrary evidence and are using this time period in an abundance of caution.

What Information Was Involved? Because we have been unable to confirm the date that the malware was placed on our website, we are notifying all customers who entered payment card information on our website between April 23, 2015 and October 26, 2017. The data elements potentially subject to unauthorized access include your: name, address, phone number, email address and credit and/or debit card information.

What We Are Doing. We take the security of your personal information very seriously. We have removed the infected code that led to the vulnerability and implemented additional security measures to reduce the likelihood of a similar incident from happening in the future. We are providing notice of this incident to those who may be impacted so that they can take steps to prevent against possible fraud, should they feel it is necessary to do so. We will also notify any required state regulators and the credit reporting agencies about this incident.

What You Can Do. You can stay vigilant by reviewing your credit card statements for any suspicious charges. You can also review the enclosed *Steps You Can Take to Protect Against Identity Theft and Fraud* which includes guidance on steps you can take to better protect against the possibility of fraud and identify theft.

For More Information. If you have questions or concerns that are not addressed in this notice letter, you may call the confidential call center we have set up for this matter at 1-855-861-4023 Monday through Saturday, 9:00 a.m. to 9:00 p.m. E.T.

We take the privacy of your personal information seriously. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

Catherine Bailey

Catherine Bailey
President & COO

Steps You Can Take to Protect Against Identity Theft and Fraud

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.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised 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 bureau with a valid police report, it cannot charge you to place, list or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
1-800-685-1111	1-888-397-3742	1-888-909-8872
(NY residents please call 1-800-349-9960)	www.experian.com/freeze/center.html	www.transunion.com/credit-freeze
https://www.freeze.equifax.com		

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting 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. **For Maryland residents**, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. **For North Carolina residents**, the Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov. **For Rhode Island Residents:** The Rhode Island Attorney General may be contacted at: Rhode Island Attorney General's Office, 150 South Main St., Providence, RI 02903. http://www.riag.ri.gov. Approximately 61 Rhode Island residents may have been affected by this incident. **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. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.