LEWIS BRISBOIS BISGAARD & SMITH LLP

Alyssa R. Watzman
1700 Lincoln Street, Suite 4000
Denver, Colorado 80203
Alyssa.Watzman@lewisbrisbois.com
Direct: 720.292.2052

October 26, 2018

VIA ELECTRONIC SUBMISSION

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

Re: Notification of Data Security Incident

Dear Attorney General Foster:

We represent Hairbow Center, LLC ("Hairbow") in connection with a recent data security incident which is described in greater detail below. Hairbow takes the security and privacy of the personal information in its control very seriously and is taking steps to prevent a similar incident from occurring in the future.

1. Nature of the security incident.

On September 26, 2018, Hairbow learned of a potential data security incident that may have affected payment card information belonging to its customers. Specifically, Hairbow was informed by Shopper Approved, LLC ("Shopper"), a third party vendor that provides rating and review services, that a malicious actor modified computer code maintained by Shopper and linked to an image of the Shopper seal which Hairbow displayed on its website. The modified computer code was designed to capture payment card information entered on the Hairbow website and was active from 12:35 a.m. EDT on September 15, 2018 to 11:00 a.m. EDT on September 17, 2018.

Upon learning of this incident, Hairbow immediately removed the Shopper seal from its website. In addition, Shopper removed the modified computer code and launched an investigation. Shopper also engaged a leading cybersecurity investigation firm to assist with the investigation and began taking steps to enhance the company's security posture. Finally, Shopper also contacted law enforcement and will cooperate with any investigation of this incident.

2. Number of New Hampshire residents affected.

Hairbow notified four (4) New Hampshire residents regarding this data security incident. Notification letters were mailed via first class U.S. mail earlier this week. A sample copy of the letter is included.

3. Steps taken relating to the incident.

Hairbow 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 in its possession. These steps include removing the Shopper image from its website and working with Shopper as it completes an investigation in order to determine what happened and the information potentially accessed.

4. Contact information.

Hairbow is dedicated to protecting the sensitive information that is in its control. If you have any questions or need additional information, please do not hesitate to contact me at (720)292-2052, or by e-mail at Alyssa.Watzman@LewisBrisbois.com.

Sincerely,

/s/ Alyssa R. Watzman

Alyssa R. Watzman of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure

HairBow Center
the supply store

<<Date>>

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

Subject: Notice of Data Breach

Dear <<First Name>> <<Last Name>>:

HairBow Center, LLC ("Hairbow") recently became aware of a potential data security incident affecting payment card information belonging to certain Hairbow customers. Hairbow takes the privacy and security of all customer information very seriously and regrets any concern that this incident may cause you. We are providing this notice to inform you of the incident and to call your attention to some steps you can take to help protect yourself.

What Happened

On September 26, 2018, we were informed of a potential data security incident by Shopper Approved, LLC ("Shopper"), a third party vendor that provides rating and review services to HairBow. According to Shopper, a malicious actor modified computer code maintained by Shopper and contained on the Shopper system which is linked to an image of the Shopper seal. At the time of the incident, we displayed that image on our website. The modified computer code was designed to capture payment card information entered on certain pages on our website. As a result of its inclusion in the Shopper image, the modified code was active on our website between 12:35 a.m. EDT on September 15, 2018 and 11:00 a.m. EDT on September 17, 2018.

What Information Was Involved

We believe that this data security incident may have affected payment information belonging to certain Hairbow customers including names, card numbers, expiration dates, and security codes. The computer code involved in this incident was designed to capture information that was typed into certain pages on our website. It did not capture information that was already stored in our systems and we do not store payment card information.

What We Are Doing

Upon learning of this incident, Shopper promptly launched an investigation and removed the code designed to capture payment card information on our website. Shopper also engaged a leading cybersecurity investigation firm to assist with the company's investigation, and is continuing to review and enhance the company's security measures to help prevent something like this from happening again in the future. Shopper also contacted law enforcement and will continue to cooperate with any investigation of this incident. As soon as we learned of this incident, we removed the Shopper image from our website.

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.

We urge you to remain vigilant and continue to monitor statements for unusual activity going forward. If you see anything you do not recognize, you may also notify proper law enforcement authorities

Other Important Information

Further information about how to protect your personal information appears on the following page. If you have questions please call 620-223-9898.

Thank you for your loyalty to Hairbow 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,

Trent Banwart

Trent Banwart, CEO
Hairbow Center, LLC

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
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-877-322-8228
www.transunion.com

Free Annual Report
P.O. Box 105281
Atlanta, GA 30348
1-877-322-8228
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.