NORTON ROSE FULBRIGHT

April 9, 2020

Via Mail

Norton Rose Fulbright US LLP
1301 Avenue of the Americas
New York, NY 10019-6022
United States

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capital Street
Concord, NH 03301

David Kessler
Partner
Direct line 215 704 5580
david.kessler@nortonrosefulbright.com

Tel +1 212 318 3382
nortonrosefulbright.com

Re: Legal Notice of Potential Information Security Incident

Dear Sirs or Madams:

We write on behalf of our client, Bimba LLC ("Bimba"), to notify you of a security incident that may have resulted in the unauthorized access or acquisition of the personal information of 15 New Hampshire residents.

We were recently informed by our vendor that our third-party cloud service provider had a vulnerability on the server that hosted our website, Bimba.com. The vulnerability did not originate from our systems but from that of a third party. As a result of this vulnerability, an unauthorized user may have been able to access or acquire personal information of our customers.

Upon learning of the incident, we immediately began an investigation and engaged a cybersecurity and forensic firm to determine how the security incident occurred and the scope of such incident. We also asked our vendor for additional information to enable us to fully investigate the incident. Our vendor informed us that they took measures to contain and remediate the vulnerability that caused the incident.

Based on the information we have to date, the unauthorized user inserted malicious code into web files causing unencrypted copies of e-commerce transaction data to be diverted to the unauthorized user. As a result, the unauthorized user may have received personal information during timeframes beginning no earlier than December 24, 2019 and no later than March 11, 2020. While the investigation is ongoing, our vendor informed us that during this timeframe, 944 individuals including 15 New Hampshire residents made transactions on Bimba.com. We intend to notify these affected individuals by April 15, 2020.

The personal information potentially access or acquired by the unauthorized user includes customer name, customer address, credit card number, expiration date, and security number for each of the transactions that occurred during the timeframe.

We are conducting a thorough review of the potentially affected records and continue to create and implement additional security measures, internal controls, and safeguards, as well as continue to make changes to existing policies and procedures designed to prevent a similar occurrence from happening again. Our vendor has informed us that no further issues can affect

NORTON ROSE FULBRIGHT

our files and they are monitoring the site daily. We are also working closely with payment card companies regarding this matter.

In addition, to help protect the identity of impacted individuals, we are offering a complimentary one-year membership of Experian's® IdentityWorks℠. This product provides superior identity detection and resolution of identity theft.

If you have any questions or need further information regarding this incident, please contact me (212) 318 3382 or david.kessler@nortonrosefulbright.com.

Very truly yours,

/s/

David Kessler

CC

Enclosure

Bimba
25150 S Governors Highway
University Park, IL 60484

Tel: +1 708 534 8544

www.bimba.com

April 15, 2020

Address
Address
Address

RE: Notice of Potential Information Security Incident

Dear [individual]:

We are writing to let you know about a data security incident involving your personal information. Bimba LLC ("Bimba") takes the protection and proper use of your information very seriously. We are therefore contacting you directly to explain the incident and provide you with steps you can take to protect yourself.

What Happened
We were recently informed by our vendor that our third-party cloud service provider had a vulnerability on the server that hosted our website, Bimba.com. The vulnerability did not originate from our systems but from that of a third party. As a result of this vulnerability, an unauthorized user may have been able to access or acquire personal information of our customers.

Upon learning of the incident, we immediately began an investigation and engaged a cybersecurity and forensic firm to determine how the security incident occurred and the scope of such incident. We also asked our vendor for additional information to enable us to fully investigate the incident. Our vendor informed us that they took measures to contain and remediate the vulnerability that caused the incident.

Based on the information we have to date, the unauthorized user inserted malicious code into web files causing unencrypted copies of e-commerce transaction data to be diverted to the unauthorized user. As a result, the unauthorized user may have received your personal information during timeframes beginning no earlier than December 24, 2019 and no later than March 11, 2020. While the investigation is ongoing, we encourage you to take the preventative measures outlined in this letter to help protect your information.

What Information Was Involved
The personal information potentially access or acquired by the unauthorized user includes your name, address, credit card number, expiration date, and security number.

What We Are Doing
We are notifying you so that you can take immediate action to protect yourself. We take the protection of your information very seriously. We are conducting a thorough review of the potentially affected records and continue to create and implement additional security measures, internal controls, and safeguards, as well as continue to make changes to existing policies and procedures designed to prevent a similar occurrence from happening again. Our vendor has informed us that no further issues can affect our files and they are monitoring the site daily. We are also working closely with payment card companies regarding this matter.

In addition, to help protect the identity of impacted individuals, we are offering you a complimentary one-year membership of Experian's® IdentityWorks℠. This product provides superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

We make things MOVE

- Ensure that you **enroll by**: **[enrollment end date]** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [URL]
- Provide your **activation code**: **[code]**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please see the enclosure or contact Experian's customer care team at [customer service number] by **[enrollment end date]**. Be prepared to provide engagement number **[engagement #]** as proof of eligibility for the identity restoration services by Experian.

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

What You Can Do
Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to protect your identity, including recommendations by the Federal Trade Commission ("FTC") regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. We also recommend you remain vigilant and promptly report any suspicious activity or suspected identity theft related to you to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the FTC.

For More Information
We sincerely apologize for this incident, regret any inconvenience it may cause you, and encourage you to take advantage of the product outlined herein. Should you have any further questions or concerns regarding this matter and/or the protections available to you, please do not hesitate to contact Nick Hajewski at 1-800-442-4622. Protecting your information is important to us.

We trust that the services we are offering to you demonstrated our continued commitment to your security and satisfaction. See the enclosed "Additional Information" for additional important information.

Sincerely,

Nick Hajewski
Communications Lead

Additional Information
A credit card is **not** required for enrollment in Experian IdentityWorks. You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.

IMI
Precision Engineering

- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at [customer service number]. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Contact information for the three nationwide credit reporting companies:

Equifax	Experian	TransUnion
Phone: 1-800-685-1111	Phone: 1-888-397-3742	Phone: 1-888-909-8872
P.O. Box 740256	P.O. Box 9554	P.O. Box 105281
Atlanta, Georgia 30348	Allen, Texas 75013	Atlanta, GA 30348-5281
www.equifax.com	www.experian.com	www.transunion.com

Free Credit Report. We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too. How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze

within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

Don't confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

For New Mexico residents: You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

For Colorado and Illinois residents: You may obtain information from the credit reporting agencies and the FTC about security freezes.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. As of September 18, 2018 when you place a fraud alert, it will last one year, instead of 90 days. Fraud alerts will still be free and identity theft victims can still get an extended fraud alert for seven years.

For Colorado and Illinois residents: You may obtain additional information from the credit reporting agencies and the FTC about fraud alerts.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland Residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Rhode Island Residents: You have the right to file or obtain a police report regarding this incident. You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov, 401-274-4400.

Reporting of identity theft and obtaining a police report. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.