



2049 Century Park East, Suite 2900, Los Angeles, CA 90067 • (310) 229-1335

July 17, 2023

Pasha Sternberg
Principal
310.229.1335
psterberg@polsinelli.com

VIA E-MAIL (IDTHEFT@OAG.STATE.MD.US)

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Notification of a Data Security Incident

Dear Madam/Sir:

We represent J&D Brush Co. LLC dba Bio Ionic (“Bio Ionic”), located at 5 Adams Avenue, Hauppauge, New York 11788, in connection with an incident that may have involved the personal information of thirty-seven (37) Maryland residents. Bio Ionic is reporting the incident pursuant to MD. CODE ANN., COM. LAW § 14-3504(H). This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to this submission. While Bio Ionic is notifying you of this Incident, Bio Ionic does not waive any rights or defenses relating to the incident or this notice, or the applicability of Maryland law on personal jurisdiction.

NATURE OF THE INCIDENT

Upon discovering that its website contained unauthorized code, Bio Ionic began an internal investigation, notified law enforcement, and through its counsel engaged a leading computer forensics firm to investigate the incident and confirm the security of its website and computer systems. Through that forensic investigation, it was determined that an unauthorized code was placed into the Bio Ionic website, which allowed an unknown, unauthorized third party to potentially view and capture certain information that was entered into the website’s checkout page as consumers made purchases through the website between March 7, 2023, and March 27, 2023.

polsinelli.com

Atlanta	Boston	Chicago	Dallas	Denver	Houston	Kansas City	Los Angeles	Miami	Nashville	New York
Phoenix	St. Louis	San Francisco	Seattle	Silicon Valley	Washington, D.C.	Wilmington				

Polsinelli PC, Polsinelli LLP in California



July 17, 2023

Page 2

The information the code would have gathered included an individual's name, shipping and billing addresses, payment card information, and email address.

NOTIFICATION TO THE MARYLAND RESIDENTS

Bio Ionic determined that the information potentially viewed or captured contained the personal information of thirty-seven (37) Maryland residents. Bio Ionic mailed notification letters to these individuals via US First Class mail on July 17, 2023. Enclosed is a sample of the notice sent to the Maryland residents.

STEPS TAKEN RELATING TO THE INCIDENT

Upon discovering the incident, Bio Ionic initiated an internal investigation, notified law enforcement, and engaged a leading forensic cybersecurity firm to assist in its investigation and to confirm the security of its website and computer systems. In addition, Bio Ionic is also working with the credit card brands to address the issue. As discussed above, Bio Ionic is notifying the potentially involved individuals, providing information on how they can protect themselves against fraudulent activity and identity theft. Finally, Bio Ionic is reviewing its information security policies and evaluating additional controls it can implement to reduce the risk of a similar incident occurring in the future.

CONTACT INFORMATION

Please do not hesitate to contact me if you have any questions or if I can provide you with any further information concerning this matter.

Sincerely,

Pasha Sternberg
Principal

Enclosure



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

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

RE: NOTICE OF DATA BREACH

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

J&D Brush Co. LLC dba Bio Ionic ("Bio Ionic" or "we") is committed to the privacy of individuals and takes the protection of personal information that is entrusted to us seriously. That is why we are writing to advise you of a recent incident that may have involved some of your personal information. This letter provides additional information about the incident and guidance on what you can do to protect yourself, should you feel it is appropriate to do so.

What Happened? On March 27, 2023, we learned that our website contained code that Bio Ionic had not approved. Upon identifying the issue, we promptly began an internal investigation and engaged a forensic security firm to conduct a further investigation. The investigation determined that the code allowed a third party to view and potentially capture information that was entered on our checkout page as customers made purchases on the website between March 7th and 27th, 2023.

What Information Was Involved? Based on our investigation, information entered into the website's checkout page including your name, shipping address, payment card information, and email address.

What We Are Doing. In addition to the steps described above, we have notified law enforcement. We are also working with the credit card brands to address the issue. Finally, we have updated our website's infrastructure to reduce the likelihood of this type of incident occurring in the future.

What You Can Do. It is generally recommended that you review your credit card statements and financial accounts for unauthorized activity. We also encourage you to review the information on steps you can take to protect yourself against possible identity theft or fraud, which is included in the enclosed *Additional Important Information* sheet.

For More Information. We value the trust you place in us to protect your information, take our responsibility to safeguard your information seriously, and apologize for any inconvenience or concern this incident might cause. For further information and assistance, please call [TFN](#) between 9:00 a.m. and 6:30 p.m. Eastern Time, Monday through Friday, excluding some U.S. holidays.

Sincerely,

Francesca Raminella
CEO

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring 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 incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, 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 print a copy of the request form at <https://www.annualcreditreport.com/manualRequestForm.action>.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax
1-866-349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
1-888-397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion
1-800-888-4213
www.transunion.com
P.O. Box 2000
Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze can be placed without any charge and is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze
1-888-298-0045
www.equifax.com
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
1-888-397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
1-888-909-8872
www.transunion.com
P.O. Box 160
Woodlyn, PA 19094

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and
7. 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.

The credit reporting agencies have three (3) 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 (5) 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 security freeze in order 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 or, if available, comply with the consumer reporting agencies' online procedures for lifting a security freeze, 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 as well as 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 (3) 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, you must send a written request to each of the three credit bureaus by mail or, if available, comply with the consumer reporting agencies' online procedures for removing a security freeze, 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 (3) business days after receiving your request to remove the security freeze.

This notification was not delayed by law enforcement.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfrp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

District of Columbia Residents: District of Columbia residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at 441 4th Street, NW, Washington, DC 20001, 202-727-3400, oag@dc.gov, <https://oag.dc.gov/>. The District of Columbia law also allows consumers to place a security freeze on their credit reports without any charge.

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, <http://www.marylandattorneygeneral.gov/>.

Massachusetts: Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. Massachusetts law also allows consumers to place a security freeze on their credit reports without any charge.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; <https://ag.ny.gov/consumer-frauds/identity-theft>; (800) 771-7755.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.

Rhode Island Residents: We believe that this incident affected 9 Rhode Island residents. Rhode Island residents can contact the Office of the Attorney general at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).