



150 N. Riverside Plaza, Suite 3000, Chicago, IL 60606 • (312) 819-1900

November 15, 2024

Michael J. Waters
(312) 463-6212
(312) 873-2918 Direct Fax
mwaters@polsinelli.com

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

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

Re: Notification of a Potential Data Security Incident

To Whom It May Concern:

We represent TriLink BioTechnologies LLC (“TriLink”) in connection with a recent incident that may have affected the personal information of one (1) Maryland resident and are reporting a potential data security 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 its submission. While TriLink is notifying you of this incident, TriLink 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 SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS

TriLink is a biotechnology company that is based in San Deigo, California. TriLink recently identified malicious code on the Product Order page of its website that may have allowed someone to scrape payment card information. TriLink promptly took steps to remove the code and secure its website. TriLink also conducted an investigation and determined that the code could have scraped payment card information related to purchases placed between September 11-14, 2024.

NUMBER OF MARYLAND RESIDENTS AFFECTED

On November 12, 2024, TriLink identified nine (9) individuals, including one (1) Maryland resident, who used payment cards during the relevant time. The information at issue includes name and payment card information. TriLink is mailing notification letters to the involved cardholders today. A copy of the notice to the involved individuals is enclosed.

polsinelli.com

Atlanta Boston Chicago Dallas Denver Houston Kansas City Los Angeles Nashville New York Phoenix
St. Louis San Francisco Seattle Washington, D.C. Wilmington
Polsinelli PC, Polsinelli LLP in California

99897174.1



November 15, 2024

Page 2

STEPS TAKEN RELATING TO THE INCIDENT

Upon learning of the incident, TriLink promptly launched an internal investigation and took steps to contain the incident. TriLink also notified law enforcement and the card brands. TriLink also has taken steps to update its website to reduce the risk of a similar incident occurring in the future.

CONTACT INFORMATION

Please contact me if you have any questions or if I can provide you with any further information concerning this matter.

Very truly yours,

Michael J. Waters

Enclosure



November 15, 2024

<<First Name>><<Last Name>>
<<Address>>
<<City>><<State>><<Zip Code>>

Dear <<First Name>><<Last Name>>,

Re: NOTICE OF A DATA BREACH

TriLink BioTechnologies LLC (“TriLink”) values and respects the security of your information, which is why we are writing to advise you a recent incident that may have involved your payment card information. This letter explains the incident, the steps we have taken in response, and provides information on steps you may take to help protect your information, should you feel it is appropriate to do so.

What Happened? We recently discovered that someone inserted malicious code on the product order page of TriLink’s website (www.trilinkbiotech.com/quickorder). In response, we promptly took steps to secure the site and identify transactions placed during the period in which the code was present.

What Information Was Involved? On November 12, 2024, we determined that you placed an order on the site during the relevant period and, as such, someone could have acquired information about the payment card you used to make a purchase on the site, including the payment card number.

What We Are Doing. In addition to taking steps to secure the website, we notified law enforcement as well as the payment card brands.

What You Can Do. While the situation has been remediated and we have no evidence that your personal information was misused, we have provided with this letter additional information on steps you can take to protect yourself against the misuse of your information.

For More Information. For further information and assistance, please call our legal department at [REDACTED] from 9 a.m. – 5 p.m. PST, Monday through Friday, excluding bank holidays.

Sincerely,

TriLink

Additional Important Information

Monitor Your Accounts

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 payment card 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 have rights under the Fair Credit Reporting Act (FCRA), which governs the collection and use of information about you by consumer reporting agencies. For more information about your rights under the FCRA, please visit <https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act>.

Credit Freeze

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the addresses below or, if available, comply with the consumer reporting agencies' online security freeze request procedures:

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.

Credit Reports: We recommend that you periodically obtain your credit report from one or more of the national credit reporting companies. You can obtain a free credit report 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 follows:

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.

Important Contacts: To access your credit report, or to implement a security freeze or a fraud alert, you may contact the three major credit reporting agencies listed below.

	Access your Credit Report	Implement a Security/Credit Freeze	Implement a Fraud Alert
Equifax	P.O. Box 740241 Atlanta, GA 30374-0241 1-866-349-5191 equifax.com/personal/credit-report-services/	P.O. Box 105788 Atlanta, GA 30348-5788 1-888-298-0045 equifax.com/personal/credit-report-services/	P.O. Box 105069 Atlanta, GA 30348-5069 1-800-525-6285 equifax.com/personal/credit-report-services/
Experian	P.O. Box 2002 Allen, TX 75013-9701 1-866-200-6020 experian.com	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 experian.com/freeze/center.html	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 experian.com/fraud/center.html
TransUnion	P.O. Box 1000 Chester, PA 19016-1000 1-800-888-4213 transunion.com	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 transunion.com/credit-freeze	P.O. Box 2000 Chester, PA 19016-2000 1-800-680-7289 transunion.com/fraud-alerts

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. Please note this notice was not delayed at the request of law enforcement.

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/>.