

RECEIVED

JUL 20 2020

CONSUMER PROTECTION

BakerHostetler

Baker & Hostetler LLP

11601 Wilshire Boulevard
Suite 1400
Los Angeles, CA 90025-0509

T 310.820.8800
F 310.820.8859
www.bakerlaw.com

M. Scott Koller
direct dial: 310.979.8427
mskoller@bakerlaw.com

July 16, 2020

VIA OVERNIGHT MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General MacDonald:

We are writing on behalf of our client, Pharmavite LLC (“Pharmavite”), to provide notice of a security incident involving four (4) New Hampshire residents.

On July 6, 2020, Pharmavite learned that an unauthorized actor had accessed an employee’s email account at various times between June 12, 2020 and June 15, 2020. As soon as it became aware of suspicious activity, Pharmavite took immediate measures to secure the email account and launched a thorough investigation to determine who was impacted and what information may have been affected. Based on this investigation, it was determined that some personal information was potentially accessible, including names, addresses, and driver’s license and social security numbers.

Beginning on July 9, 2020, Pharmavite began mailing notification letters via United States Postal Service First-Class mail to four (4) New Hampshire residents in accordance with N.H. Rev. Stat. Ann. § 359-C:20. A copy of the notification letter is enclosed.¹ Pharmavite has provided a telephone number for potentially affected individuals to call with any questions they may have and has offered these individuals a complimentary two-year membership to Experian’s IdentityWorks credit monitoring service.

¹ This report is not, and does not constitute, a waiver of the Pharmavite’s objection that New Hampshire lacks personal jurisdiction over Pharmavite regarding this incident.

Atlanta Chicago Cincinnati Cleveland Columbus Costa Mesa Denver
Houston Los Angeles New York Orlando Philadelphia Seattle Washington, DC

To help prevent something like this from happening in the future, Pharmavite is taking steps to enhance its existing security protocols and is reeducating its staff for awareness on these types of incidents. It has also notified law enforcement of the incident.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

M. Scott Koller

M. Scott Koller

Enclosures



PHARMAVITE

July 9, 2020

First and Last Name

Street Address

City, State, Zip Code

Notice of Data Breach

Dear [First Name] [Last Name],

At Pharmavite LLC ("Pharmavite"), protecting the security and confidentiality of your personal information is of the utmost importance. Regrettably, we are writing to inform you about an incident involving some of your information. This notice describes the incident, outlines the measures we have taken in response, and offers options for you to further protect your information.

What Happened?

We recently conducted an investigation into suspicious activity originating from unauthorized access to an employee's email account. As soon as we became aware of the suspicious activity, we immediately took measures to secure the email account and launched an internal investigation. The investigation determined that an unauthorized person had accessed an employee's email account at various times from June 12 to June 15, 2020. On July 7, 2020, we concluded our investigation, determining that the email account contained personal information that was potentially accessible.

What Information Was Involved?

The investigation was not able to determine whether any specific emails were accessed by the unauthorized person; however, we were not able to rule out that possibility. Out of an abundance of caution, we conducted a thorough review of all emails and attachments that were potentially accessible. We are notifying you because the email account contained a message or attachment with your personal information, including your name, address, and social security number.

What We Are Doing.

To further protect personal information, we are taking steps to enhance our existing security protocols and re-educating our staff for awareness on these types of incidents. We have notified law enforcement of the incident.

What You Can Do.

Even though we have no indication that your information has been misused, we encourage you to remain vigilant for incidents of fraud or identity theft by reviewing your account statements for any unauthorized activity. Out of an abundance of caution, we are offering a complimentary two-year membership to Experian's® IdentityWorks Credit 360. This product helps detect possible misuse of your personal information and provides you with identity protection

services focused on identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate the complimentary membership, please see the additional information provided with this letter.

For More Information.

We deeply regret any inconvenience this incident may cause you. For more information, please contact our dedicated call center at 844-951-2880, Monday through Friday from 8am until 5:30pm Central Time (6am to 3:30pm Pacific).

Sincerely,

Christine Burdick-Bell

Executive Vice President, General Counsel & Corporate Secretary

Pharmavite LLC

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **9.30.2020** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the **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 contact Experian's customer care team at 877-288-8057. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **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.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at <https://www.experianidworks.com/3bcredit>

or call 877-288-8057 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable 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. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

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 state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report. For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com

- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

Connecticut: You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us