

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

June 28, 2021

VIA E-MAIL (DOJ-CPB@DOJ.NH.GOV)

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

Re: Incident Notification

Dear Attorney General Gordon MacDonald:

We are writing on behalf of our client, Pharmavite LLC (“Pharmavite”) to notify you of a security incident involving three New Hampshire residents. Pharmavite is headquartered in Northridge, California.

Pharmavite recently conducted an investigation into suspicious activity originating from unauthorized access to an employee’s email account. Upon discovering the incident, Pharmavite immediately took steps to secure the email account, and began an internal investigation. The investigation determined that an unauthorized person had accessed an employee’s email account on April 6, 2021. Pharmavite concluded the investigation, determining that the email account contained personal information that was potentially accessible. The investigation could not determine whether any specific emails were accessed by the unauthorized person; however, Pharmavite was not able to rule out that possibly. Out of an abundance of caution, Pharmavite conducted a thorough review of all emails and attachments that were potentially accessible, and on May 10, 2021, Pharmavite’s investigation determined that the email account contained a message or attachment pertaining to three New Hampshire residents, including the individuals’ names and Social Security numbers.

Beginning today, June 28, 2021, Pharmavite is providing written notice to the New Hampshire residents by mailing a letter via United States Postal Service First-Class mail.¹ A sample copy of the notification letter is enclosed. Pharmavite is offering the New Hampshire residents whose SSN

¹ This report does not waive Pharmavite’s objection that New Hampshire lacks personal jurisdiction over it related to any claims that may arise from this incident.

June 28, 2021

Page 2

may have been involved a complimentary, two-year membership to credit monitoring and identity theft prevention services through Experian. Pharmavite is recommending that the affected individuals remain vigilant to the possibility of fraud by reviewing their account statements for unauthorized activity. Pharmavite has also established a dedicated phone number where the individual may obtain more information regarding the incident.

To further protect personal information, Pharmavite is rolling out significant changes to its already existing security protocols, particularly around storage of emails, with companywide upgrades soon to be announced. Pharmavite is also continuing education efforts with its staff to ensure they are aware of these types of continuously evolving incidents.

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

Sincerely,

A handwritten signature in cursive script that reads "M. Scott Koller".

M. Scott Koller
Partner

Enclosure



PHARMAVITE

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

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

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 potentially 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 on April 6, 2021. On May 10, 2021, we concluded our investigation, determining that the email account contained personal information that was potentially accessible.

What Information Was Involved?

The investigation could not 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 <<b2b_text_1(DataElements)>>.

What We Are Doing.

To further protect personal information, we are rolling out significant changes to our existing security protocols, particularly around storage of emails, with companywide upgrades soon to be announced. We are continuing education efforts with our staff to ensure they are aware of these types of continuously evolving incidents.

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. It is also advisable to review the billing statements you receive from your health insurer or healthcare provider. If you see charges for services that you did not receive, please contact the insurer or provider immediately. Out of an abundance of caution, we are offering a complimentary two-year membership to Experian's® IdentityWorks Credit 3B. 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. If you already have IdentityWorks Credit 3B this complimentary membership will add an additional two years of monitoring.

For More Information.

We deeply regret any inconvenience this incident may cause you. For more information, please contact our dedicated call center at 1-855-731-3329, Monday through Friday from 8:00 a.m. until 5:30 p.m. Central Time (6:00 a.m. to 3:30 p.m. Pacific), excluding some U.S. holidays.

Sincerely,

Christine Burdick-Bell

Christine Burdick-Bell
Executive Vice President, General Counsel & Corporate Secretary
Pharmavite LLC

EXPERIAN'S® IDENTITYWORKSSM CREDIT 3B ENROLLMENT INSTRUCTIONS

To help protect your identity, we are offering a **complimentary** two-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: <<b2b_text_2(EnrollmentDeadline)>> (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**: <<Member ID>>

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 <<b2b_text_3(EngagementNumber)>> 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.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. 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

District of Columbia: You may contact and obtain information from your attorney general at: *Office of the Attorney General for the District of Columbia*, 441 4th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov

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

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Rhode Island: This incident involves one individual in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.