

McDonald Hopkins

A business advisory and advocacy law firm®

McDonald Hopkins PLC
100 International Drive
23rd Floor
Baltimore, MD 21202

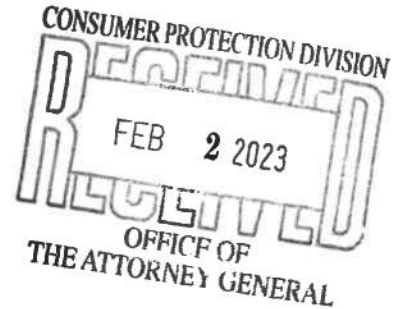
P 1.410.917.5189

Spencer S. Pollock, CIPP/US, CIPM
Direct Dial: 1.410.456.2741
Cell: 1.410.917.5189
Email: spollock@mcdonaldhopkins.com

January 26, 2023

VIA U.S. MAIL

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



Re: Pharmaceutical Specialties, Inc. – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents Pharmaceutical Specialties, Inc. (“Pharmaceutical Specialties”). I am writing to provide notification of an incident at Pharmaceutical Specialties that may affect the security of personal information of approximately one (1) Maryland resident. Pharmaceutical Specialties’ investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, Pharmaceutical Specialties does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Pharmaceutical Specialties recently discovered unauthorized access to its network occurred between approximately June 21, 2022 and June 24, 2022. Pharmaceutical Specialties immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to analyze the extent of any compromise of the information on its network. Based on its comprehensive investigation and document review, which concluded on January 16, 2023, Pharmaceutical Specialties discovered that a limited amount of personal information may have been removed from its network in connection with this incident, including the affected resident’s full name and financial account information.

To date, Pharmaceutical Specialties is not aware of any reports of identity fraud or improper use of any information as a direct result of this incident. Nevertheless, out of an abundance of caution, Pharmaceutical Specialties wanted to inform you (and the affected resident) of the incident and to explain the steps that it is taking to help safeguard the affected resident against identity fraud. Pharmaceutical Specialties is providing the affected resident with written notification of this incident commencing on or about January 27, 2023 in substantially the same

Baltimore | Chicago | Cleveland | Columbus | Detroit | West Palm Beach

mcdonaldhopkins.com

{10934230: }

form as the letter attached hereto. Pharmaceutical Specialties is advising the affected resident about the process for placing fraud alerts and/or security freezes on his/her credit files and obtaining free credit reports. The affected resident is being advised to contact his/her financial institution(s) to inquire about steps to take to protect his/her account(s). The affected resident is also being provided with the contact information for the consumer reporting agencies, the Federal Trade Commission, and the Maryland Attorney General.

At Pharmaceutical Specialties, protecting the privacy of personal information is a top priority. Pharmaceutical Specialties is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Pharmaceutical Specialties continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information.

Should you have any questions regarding this notification, please contact me at 410.456.2741 or spollock@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,

A handwritten signature in black ink, appearing to read 'Spencer S. Pollock', with a stylized, cursive script.

Spencer S. Pollock

Encl.

Pharmaceutical Specialties, Inc.

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]



**IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY**

[REDACTED]
[REDACTED]
[REDACTED]



Dear [REDACTED]

We are writing with important information regarding a recent security incident. The privacy and security of the personal information we maintain is of the utmost importance to Pharmaceutical Specialties, Inc. We wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

We recently discovered unauthorized access to our network occurred between approximately June 21, 2022 and June 24, 2022.

What We Are Doing.

We immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to analyze the extent of any compromise of the information on our network.

What Information Was Involved?

Based on our comprehensive investigation and document review, which concluded on January 16, 2023, we discovered that your full name and one or more of the following may have been removed from our network in connection with this incident: [REDACTED].

What You Can Do.

To date, we are not aware of any reports of identity fraud or improper use of your information as a direct result of this incident. Out of an abundance of caution, we wanted to make you aware of the incident, explain the services we are making available to help safeguard you against identity fraud, and suggest steps that you should take as well. We are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and/or Security Freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line [REDACTED] and supply the fraud specialist with your unique code listed above.

Sincerely,

Pharmaceutical Specialties, Inc.

1620 Industrial Dr. NW

Rochester, MN 55901

- OTHER IMPORTANT INFORMATION -

1. Enrolling in Complimentary 12-Month Credit Monitoring.

To enroll in Credit Monitoring services at no charge, please log on to [REDACTED] and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED] In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 12-month credit monitoring services, we recommend that you place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

3. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(888)-298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
(888) 909-8872

In order to place the security freeze, 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 reporting company will send you a confirmation letter containing 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.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: (515) 281-5164.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755 (TDD/TYY Support: 800-788-9898); Medicare Fraud Control Unit Direct Line: 212-417-5397.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.