Pharm-Pacc Corporation
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB07862 1-1

PHARM-PACC
Maximize Your Assistance Recovery

[redacted]

September 14, 2023

Subject: Notice of Data Security Incident

Dear [redacted],

I am writing to inform you of a recent data security incident experienced by Pharm-Pacc, Corporation ("Pharm-Pacc")[1] that may have affected your personal or protected health information. Pharm-Pacc takes the privacy and security of your information very seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your information.

What Happened? On March 24, 2023, Pharm-Pacc discovered suspicious activity that impacted its digital environment. In response, Pharm-Pacc took immediate steps to secure its digital environment and promptly launched a forensic investigation, aided by an independent cybersecurity firm, to determine what happened and whether any information may have been impacted. On May 23, 2023, Pharm-Pacc received confirmation that certain of its digital systems were accessed without authorization. Pharm-Pacc then engaged a vendor to conduct a comprehensive review to determine whether those systems contained any personal or protected health information. On July 14, 2023, Pharm-Pacc learned that your personal or protected health information was kept on one of its digital systems and therefore may have been impacted in connection with the incident. Pharm-Pacc then promptly notified your healthcare provider of the incident and worked diligently with them to identify up-to-date address information necessary to provide notice to you.

What Information Was Involved? The information potentially impacted in connection with this incident included your name as well as your [redacted].

What Are We Doing? As soon as Pharm-Pacc discovered this incident, it took the steps described above. In addition, Pharm-Pacc implemented measures to enhance the security of its digital environment in an effort to minimize the risk of a similar incident occurring in the future.

What You Can Do: You can follow the recommendations on the following page to help protect your information.

For More Information: Further information about how to protect your information appears on the following page. If you have questions or need assistance, please call Cyberscout at 1-833-961-5700 from 8:00 A.M. to 8:00 P.M. Eastern Time, Monday through Friday (excluding holidays). Cyberscout call center representatives are fully versed on this incident and can answer any questions that you may have.

[1] Pharm-Pacc provides managed recovery services including medication claims processing and administration for uninsured patients.

Please accept my sincere apologies and know that Pharm-Pacc takes this matter very seriously and deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

Carlos Mendia
Chief Executive Officer
Pharm-Pacc Corporation

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and 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 also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, 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 also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
ag.ny.gov
1-212-416-8433 / 1-800-771-7755

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.