CONSTANGY BROOKS, SMITH & PROPHETE LLP

Cybersecurity & Data Privacy Team
1201 Elm Street, Suite 2550
Dallas. Texas 75270

April 18, 2023

VIA E-MAIL

Attorney General John M. Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, New Hampshire 03301
E-mail: doj-cpb@doj.nh.gov

Re: **Notification of Data Security Incident**

To Attorney General Formella:

We represent Professional Compounding Centers of America, Inc. ("PCCA") in connection with a recent data security incident described below. PCCA is notifying affected individuals of the incident. The purpose of this letter is to provide formal notice to your office.

I. Nature of the Security Incident

On February 8, 2023, PCCA discovered unusual activity within its digital environment. Upon discovery, PCCA took immediate steps to secure the environment. In addition, PCCA retained an independent third-party computer forensic investigator to conduct an investigation to determine what happened. The forensic investigation revealed that an unauthorized actor gained access to the PCCA network, and that some personal information may have been acquired without authorization in connection with the incident. The information may have included . PCCA worked diligently to confirm the identity of the potentially affected individuals and obtain updated address information to provide notification to individuals. This process was completed on April 7, 2023.

II. Number of New Hampshire Residents Affected

Based on PCCA's investigation, a total of two (2) residents of New Hampshire may have had information acquired without authorization during the incident. Notification letters were sent to these individuals via first class U.S. mail on April 18, 2023. A sample copy of that notification letter is enclosed.

III. Actions Taken in Response to the Incident

As soon as PCCA became aware of the potential incident, it launched an investigation, took immediate steps to enhance the security of its network, and worked to determine whether any personal information was accessed or acquired without authorization. PCCA then worked diligently to determine what personal information may have been affected, the individuals to whom the information pertained, and the addresses for those individuals to provide notification to all potentially affected individuals.

As part of the notice, PCCA is offering the New Hampshire residents with 24 months of Single Bureau

Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services, proactive fraud assistance, and a $1,000,000 insurance reimbursement policy by Cyberscout through Identity Force, a TransUnion company.

IV. Contact Information

If you have any questions or need additional information, please do not hesitate to contact me at

Sincerely,

Lindsay B. Nickle
CONSTANGY, BROOKS, SMITH & PROPHETE, LLP

Professional Compounding Centers of America, Inc.
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
«uniqueid» «ctn_no»-«pkg_no_ctn»

«firstname» «lastname»
«address1» «address2»
«city», «state» «postalcode4»-«zip4»
«imb_encode»

April 18, 2023

Re: Notice of Data «custom_field_1»

Dear «firstname» «lastname»,

We are writing to provide you with information about a recent data security incident that may have involved your personal information. At Professional Compounding Centers of America, Inc. ("PCCA"), we take the privacy and security of all information in our possession very seriously. That is why we are writing to notify you of the incident and to provide you with information about steps you can take to help protect your personal information.

What Happened. On February 8, 2023, PCCA discovered unusual activity within our digital environment. We took immediate steps to secure the environment, and retained an independent third-party computer forensic investigator to conduct an investigation to determine what happened. The forensic investigation revealed that an unauthorized actor gained access to our network. Our investigation determined that some personal information may have been acquired without authorization in connection with the incident. Based on the findings from the investigation, we undertook a thorough review of the affected systems to determine what personal information may have been impacted, the individuals to whom the information pertained, and the addresses for these individuals. This process was completed on April 7, 2023.

What Information Was Involved. The information affected may have involved your «exposed_data_elements».

What We Are Doing. As soon as we detected the incident, we took the measures discussed above. While we are unaware of any evidence that your personal information has been misused, we are also providing you with information on the following page about steps you can take to help protect your personal information. Plus, we are offering you **free credit monitoring services** for 24 months as described below.

What You Can Do. You can follow the recommendations included with this letter to protect your personal information. We also strongly encourage you to enroll in the Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services we are offering to you at no cost to you. These services provide you with alerts for 24 months from the date of enrollment when charges occur to your credit file. We are also providing you with proactive fraud assistance to help you with any questions, and a $1,000,000 insurance reimbursement policy. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services, please log on to **https://secure.identityforce.com/benefit/profcompounding** and follow the instructions provided. When prompted, please provide the following unique code to receive services: **«uniquecode».** Please note the enrollment deadline is July 18, 2023.

For More Information. If you have any questions regarding the incident, please call between 8:00 am Eastern Time to 8:00 pm Eastern Time from Monday through Friday, excluding holidays.

Please accept our sincere apologies. Know that we deeply regret any worry or inconvenience that this may have caused you.

Sincerely,

Manfredo Thibau
Chief Financial Officer

Steps You Can Take to Protect Your Personal 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
oag.state.md.us
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

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
441 4th 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://www.consumer ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.