CONSTANGY
BROOKS, SMITH & PROPHETE LLP

1650 Market Street
36th Floor
Philadelphia, Pennsylvania 19103

April 20, 2023

Via Email

Attorney General John Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Email: DOJ-CPB@doj.nh.gov

Re: Notice of Data Security Incident

Dear Attorney General Formella:

Constangy, Brooks, Smith & Prophete, LLP ("Constangy") represents Sun Pharmaceutical Industries, Inc. ("Sun Pharma") in connection with a recent Information Technology ("IT") security incident described in greater detail below.

1. **Nature of the IT security incident.**

Sun Pharma experienced an IT security incident in early March. As soon as the company discovered the incident, it promptly took steps to contain and remediate its impact, including employing containment protocols to mitigate the threat and additional measures to ensure the integrity of its IT systems infrastructure and data, as well as the retention of cyber security experts and the use of enhanced security measures.

The company believes that the incident's effect on its IT systems includes a breach of certain file systems and the theft of certain company data and personal data. While Sun Pharma does not yet know whether the information of its former and current employees was involved in the incident, and it has no evidence that anyone's data has been misused, out of an abundance of caution, it provided notification and complimentary credit monitoring to former and current employees.

The information potentially impacted in connection with this incident may include names and the identifying information that employees provided to Sun Pharma, such as

.

2. **Number of New Hampshire residents affected.**

Sun Pharma notified fifty-seven (57) New Hampshire residents of this incident via first class U.S. mail on April 19, 2023. A sample copy of the notification letters is included with this correspondence.

3. Steps taken relating to the incident.

As soon as Sun Pharma discovered this IT security incident, it launched an investigation to determine what happened and the scope of personal information potentially impacted. In addition, Sun Pharma implemented measures to enhance the security of its environment in an effort to minimize the risk of a similar incident occurring in the future.

Sun Pharma has established a toll-free call center through TransUnion, a leader in risk mitigation and response, to answer any questions about the incident and address related concerns. The call center is available at 1-833-570-3007 from 8:00 A.M. to 8:00 P.M. EST on Monday through Friday.

In addition, while Sun Pharma is not aware of the misuse of any information as a result of this incident, out of an abundance of caution, Sun Pharma is also providing complimentary credit and identity protection services to notified individuals. Sun Pharma provided all benefit-eligible current employees with credit monitoring and identity protection services for a period from March 2023 to December 2024 through IDShield. Former employees and non-benefit-eligible current employees were also offered complimentary credit and identity protection services provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services, for a period of twenty-four (24) months.

Sun Pharma also notified federal law enforcement and will assist their attempts to hold the perpetrators accountable.

4. Contact information.

Sun Pharma remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact Constangy.

Best regards,

Richard W. Goldberg
CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Enclosure: Sample Notification Letters

Sun Pharmaceutical Industries, Inc.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

[redacted]

To Enroll, Please Call:
1-833-570-3007
Or Visit:
https://secure.identityforce.com/benefit/suntaropharma
Enrollment Code: [redacted]

April 19, 2023

0000101102G0500

P

Subject: Notice of Data Security Incident

Dear [redacted],

We are writing to inform you of a data security incident that may have involved your personal information. Sun Pharmaceutical Industries, Inc. ("Sun Pharma") takes the privacy and security of personal information very seriously. This is why we are notifying you of the incident, providing you with steps you can take to help protect your personal information, and offering you the opportunity to enroll in complimentary credit monitoring and identity protection services.

What Happened? Sun Pharma experienced a cyber incident in early March. We immediately took steps to find out what happened. The investigation revealed that an unknown actor gained access to and obtained some data from our network. While we do not yet know whether the information of all of our former and current employees was involved in the incident, and we have no evidence that anyone's data has been misused, out of an abundance of caution we are providing you with this notification and complimentary credit monitoring and identity protection services.

What Information Was Involved? The information involved may include your name and the identifying information you previously provided to Sun Pharma. This is information such as

.

What We Are Doing. As soon as we discovered the incident, we took the steps referenced above. We also implemented additional security features to protect the network, including employing containment protocols to mitigate the threat and additional measures to ensure the integrity of our IT systems' infrastructure and data, as well as the retention of cyber security experts and the use of enhanced security measures to address and mitigate the impact of the incident. We notified federal law enforcement and will assist their attempts to hold the perpetrators accountable.

Additionally, we are offering you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score/Cyber Monitoring** services at no charge. These services provide you with alerts for twenty-four (24) 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. Cyber monitoring will look out for your personal data on the dark web and alert you if your personally identifiable information is found online. Finally, we are providing you with proactive fraud assistance to help with any

questions that you might have or in 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.

What You Can Do. Please review this letter carefully, along with the guidance included with this letter about additional steps you can take to protect your information. You can also enroll in the Cyberscout identity protection services, which are offered to you at no cost.

To receive credit monitoring services, you must be over the age of 18 and have established credit in the United States, have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

To enroll in Credit Monitoring services at no charge, please log on to **https://secure.identityforce.com/benefit/suntaropharma** 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. Please do not discard this letter, as you will need the Enrollment Code provided above to access services.

For More Information. If you have questions about this letter or need assistance, please call . Representatives are available Monday through Friday from 8:00 a.m. to 8:00 p.m. Eastern Time. Representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

We sincerely regret any anxiety caused by this incident.

Sincerely,

Team HR
Sun Pharmaceutical Industries, Inc.

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
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

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right 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. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

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.

Sun Pharmaceutical Industries, Inc.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

[redacted]

April 19, 2023

Subject: Notice of Data Security Incident

Dear [redacted],

We are writing to inform you of a data security incident that may have involved your personal information. Sun Pharmaceutical Industries, Inc. ("Sun Pharma") takes the privacy and security of personal information very seriously. This is why we are notifying you of the incident, providing you with steps you can take to help protect your personal information, and offering you the opportunity to enroll in complimentary credit monitoring and identity protection services.

What Happened? As you know, we experienced a cyber incident in early March. We immediately took steps to find out what happened. The investigation revealed that an unknown actor gained access to and obtained some data from our network. While we do not yet know whether the information of all of our employees was involved in the incident, and we have no evidence that anyone's data has been misused, out of an abundance of caution we previously provided you with credit monitoring and identity protection services and are now providing you with this notification letter.

What Information Was Involved? The information involved may include your name and certain identifying information you provided to Sun Pharma. This is information such as

.

What We Are Doing. As soon as we discovered the incident, we took the steps referenced above. We also implemented additional security features to protect the network, including employing containment protocols to mitigate the threat and additional measures to ensure the integrity of our IT systems' infrastructure and data, as well as the retention of cyber security experts and the use of enhanced security measures to address and mitigate the impact of the incident. We notified federal law enforcement and will assist their attempts to hold the perpetrators accountable.

Additionally, we previously provided credit monitoring and identity protection services for a period from March 2023 to December 2024 through IDShield. The IDShield services, which are free to you upon enrollment, include credit monitoring, dark web monitoring, fully managed identity recovery services, and a $1 million identity fraud protection plan. With this protection, IDShield will help you resolve issues if your identity is compromised.

What You Can Do. Please review this letter carefully, along with the guidance included with this letter about additional steps you can take to protect your information. You can also enroll in the IDShield identity protection services using the enrollment instructions previously provided to you, which are offered to you at no cost.

For More Information. If you have questions about this letter or need assistance, please call IDShield at 1-888-807-0407. IDShield representatives are available Monday through Friday from 7:00 a.m. to 7:00 p.m. Central Time. IDShield representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

Sincerely,

Team HR
Sun Pharmaceutical Industries, Inc.

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
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

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right 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. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

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.