Bristol Myers Squibb

June 30, 2023

Consumer Protection & Antitrust Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
Phone: (603) 271-3643
Fax: (603) 271-2110

Re: Security Incident Notification

To Whom It May Concern:

I am writing on behalf of Bristol Myers Squibb (BMS) to inform you of an incident that impacted the personal information of New Hampshire residents. On May 31, 2023, BMS was alerted by Progress Software Corporation that it had discovered a vulnerability in its Secure File Transfer Protocol (SFTP) tool MOVEit. BMS promptly initiated an investigation with the assistance of third-party cybersecurity experts, implemented vendor-recommended actions, and engaged U.S. law enforcement.

Based on its investigation, BMS determined on June 1, 2023 that confidential BMS data had been accessed and downloaded in an unauthorized manner as early as May 27, 2023. This data included the of five (5) New Hampshire residents and may have included their

. BMS has not identified any impact from the MOVEit vulnerability on other parts of our corporate network.

On June 29, 2023, BMS sent notice by postal mail to impacted residents. A sample copy of the notice is enclosed. In addition to providing impacted New Hampshire residents with information regarding credit reporting agencies, security freezes, fraud alerts, and other identity theft prevention tools, BMS is offering 24 months of credit monitoring and identity protection services through Experian's IdentityWorks to affected individuals, at no cost to them.

Please feel free to contact me if you have any questions or require additional information.

Kind Regards,

Adam Yoffie
Senior Corporate Counsel
Litigation & Government Investigations

Adam G. Yoffie
Senior Corporate Counsel
Litigation & Government Investigations

3551 Lawrenceville Road
Princeton, NJ 08540

Mobile +908-451-9534
adam.yoffie@bms.com

Bristol Myers Squibb™

Return Mail Processing
PO Box 999
Suwanee, GA 30024

Bristol Myers Squibb
Route 206 & Province Line Road
Princeton, New Jersey 08543

10 12568 ••SNGLP
SAMPLE A. SAMPLE - L01
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

June 29, 2023

NOTICE OF DATA BREACH

Dear Sample A. Sample:

Bristol Myers Squibb ("BMS") is writing to notify you that we recently experienced a cybersecurity event where an unauthorized actor accessed a third-party software application we use to manage documents. We are taking this matter very seriously and sincerely regret any concern it may cause you.

What Happened? On May 31, 2023, BMS was alerted by Progress Software Corporation that it had discovered a vulnerability in its Secure File Transfer Protocol (SFTP) tool MOVEit. On June 1, 2023, BMS determined that confidential BMS data had been accessed and downloaded in an unauthorized manner as early as May 27, 2023.

What Information Was Involved? The information that was accessed and downloaded includes

What We Are Doing. Upon learning that the MOVEit application was accessed by an unauthorized actor, we promptly took measures to quickly respond and investigate this issue. BMS took the application offline, implemented the vendor-recommended actions, initiated an investigation with the assistance of third-party cybersecurity experts, engaged law enforcement in the United States, and notified data protection authorities, where applicable. We also promptly patched the vulnerability. We have not identified any impact from the MOVEit vulnerability on other parts of our corporate network and BMS remains fully operational. To reduce the risk of similar events happening in the future, BMS is working to further enhance its security controls. We also have arranged for you to obtain, at no cost to you, 24 months of Experian IdentityWorks℠. Information regarding these services is included in Attachment 1 to this letter.

What You Can Do. We recommend that you remain vigilant by reviewing your account statements, signing up for the of credit monitoring we are offering at no cost to you, and monitoring the reports for signs of suspicious activity. Information about how to enroll is included in Attachment 1 to this letter. Please find additional information in Attachment 2 to this letter.

For More Information. Again, we regret any concern this incident may cause you. If you have questions or concerns regarding this matter, please contact 4, Monday through Friday, 6:00 a.m. to 8:00 p.m. PST; Saturday and Sunday, 8:00 a.m. to 5:00 p.m. PST (excluding US major holidays).

Sincerely,

Miguel Crespo
Head of IT Risk Management
Bristol Myers Squibb

Attachment 1: Credit Monitoring Services Enrollment Information

To help protect your identity, we are offering complimentary access to Experian IdentityWorks℠ for

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary . This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at . Be prepared to provide engagement number as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **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 file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related 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.

* 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.

Attachment 2: Additional Information

You should be cautious about using email to provide sensitive personal information, whether sending it yourself or in response to email requests. You should also be cautious when opening attachments and clicking on links in emails. Scammers sometimes use fraudulent emails or other communications to deploy malicious software on your devices or to trick you into sharing valuable personal information, such as account numbers, Social Security numbers, or usernames and passwords. The Federal Trade Commission (FTC) has provided guidance at https://consumer.ftc.gov/articles/how-recognizeand-avoid-phishing-scams.

You should review your financial statements and accounts for signs of suspicious transactions and activities. If you find any indication of unauthorized accounts or transactions, you should report the possible threat to local law enforcement, your State's Attorney General's office, or the FTC. You will find contact information for some of those entities below. If you discover unauthorized charges, promptly inform the relevant payment card companies and financial institutions.

Fraud Alert Information
Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

Whether or not you enroll in the credit monitoring product offered, you also have the right to place an initial fraud alert on your file at no cost. An initial fraud alert lasts one (1) year and is placed on a consumer's credit file. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven (7) years. Fraud alert messages notify potential credit grantors to verify your identification before extending credit in your name in case someone is using your information without your consent. A fraud alert can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit.

Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies. You may also contact any of the consumer reporting agencies or the FTC for more information regarding fraud alerts. The contact information for the three nationwide credit reporting agencies is:

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-766-0008
www.equifax.com/personal/credit-report-services

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Free Credit Report Information

You have rights under the federal Fair Credit Reporting Act. These include, among others, the right to know what is in your credit file; the right to dispute incomplete or inaccurate information; and the right to ask for a credit score. Under federal law, you are also entitled to one free credit report once every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or make a request online at www.annualcreditreport.com.

Even if you do not find any suspicious activity on your initial credit reports, we recommend that you check your account statements and credit reports periodically. You should remain vigilant for incidents of fraud and identity theft. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports 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 or state attorney general and file a police report. Get a copy of the report; many creditors want the information it contains to alleviate you of the fraudulent debts. You also should file a complaint with the FTC using the contact information below. Your complaint will be added to the FTC's Consumer Sentinel database, where it will be accessible to law enforcement for their investigations.

You may also contact the FTC at the contact information below to learn more about identity theft and the steps you can take to protect yourself and prevent such activity. If you are a resident of the District of Columbia, Iowa, Maryland, New York, or Oregon, you can also reach out to your respective state's Attorney General's office at the contact information below. All other residents can find information on how to contact your state attorney general at https://www.naag.org/ find-my-ag/.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1.877.FTC.HELP (382.4357) /
https://www.consumer.ftc.gov/identity-theft-and-online-security

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301
1-877-877-9392 / https://justice.oregon.gov

New York Attorney General's Office
The Capitol
Albany, NY 12224-0341
1-800-771-7755
https://ag.ny.gov/consumer-frauds-bureau/identity-theft

North Carolina Department of Justice
114 West Edenton Street
Raleigh, NC 27603
1-919-716-6400
https://ncdoj.gov/protecting-consumers/identity-theft/

Office of the Attorney General for the District of Columbia
400 6th Street NW
Washington, DC 20001
1-202-727-3400 / oag.dc.gov

Maryland Attorney General's Office
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023 / www.marylandattorneygeneral.gov

Consumer Protection Division
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, IA 50319
1-515-281-5926 / www.iowaattorneygeneral.gov

Rhode Island Office of the Attorney General
150 South Main Street
Providence, RI 02903
1-401-274-4400
https://riag.ri.gov/

Security Freeze Information
You have the right to request a free security freeze (aka "credit freeze") on your credit file by contacting each of the three nationwide credit reporting companies via the channels outlined below. When a credit freeze is added to your credit report, third parties, such as credit lenders or other companies, whose use is not exempt under law will not be able to access your credit report without your consent. A credit freeze can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. You may also contact any of the consumer reporting agencies or the FTC for more information regarding security freezes.

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348
http://www.equifax.com/personal/credit-report-services/credit-freeze/
1-800-349-9960

TransUnion Security Freeze
PO Box 2000
Chester, PA 19016
https://www.transunion.com/credit-freeze
1-888-909-8872

Experian Security Freeze
PO Box 9554
Allen, TX 75013
www.experian.com/freeze
1-888-397-3742

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

1) Full name, with middle initial and any suffixes;
2) Social Security number;
3) Date of birth (month, day, and year);
4) Current address and previous addresses for the past five (5) years;
5) Proof of current address, such as a current utility bill or telephone bill;
6) Other personal information as required by the applicable credit reporting agency;

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.