GT GreenbergTraurig

Jena M. Valdetero
Tel 312.456.1025
Fax 312.456.8435
Jena.valdetero@gtlaw.com

November 20, 2026

Attorney General John Formella
Office of the Attorney General
DOJ-CPB@doj.nh.gov

Re: Notification of Security Incident

Dear Attorney General Formella:

We represent Bausch Health Companies Inc. ("Bausch Health") located at 400 Somerset Corporate Blvd., Bridgewater, NJ 08807, and are writing to notify your office that Bausch Health notified eleven New Hampshire residents of a data security incident that impacted their personal information. While Bausch Health is notifying you of this incident, Bausch Health does not waive any rights or defenses relating to the incident, this notice, or the applicability of New Hampshire law on personal jurisdiction.

On July 1, 2026, Bausch Health identified evidence of unauthorized access to a limited number of company records, including product questions and concerns maintained by Bausch Health's pharmacovigilance department. Bausch Health immediately commenced an investigation, which included engaging third-party incident response experts to assist in determining the extent of any unauthorized activity. Bausch Health has no reason to believe the unauthorized individual continues to have access.

On October 28, 2026, the investigation was complete, and Bausch Health identified personal information contained within documents obtained by the unauthorized individual. The personal information includes individuals' names along with one or more of: Social Security Number, mailing address, email address, phone number, and limited health-related information.

Bausch Health takes the security of all information in its systems very seriously, and it has taken steps to prevent a recurrence. Among other actions, the company has increased monitoring, further improved security controls, and reinforced its systems. The company is also providing complimentary credit monitoring and identity theft services to individuals whose Social Security numbers were affected. On or about November 25, 2026, Bausch Health will begin mailing notifications to all potentially affected individuals. An example of the notification is attached.

Should you have any questions regarding this notification or other aspects of the data security incident, please contact me for any additional information.

Best Regards,



Jena Valdetero
Shareholder

Schedule A

Individual Notification Letter

400 Somerset Corporate Boulevard
Bridgewater, New Jersey 08807

908 927 1400
Bauschhealth.com

November 25, 2026

VIA US MAIL

<<FIRSTNAME>><<MIDDLE NAME>><<LAST NAME>><<SUFFIX>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>,<<STATE>> <<ZIP CODE>>

Re: **<<VARIABLE 1>>**

Dear Customer,

We are writing to inform you of a recent cybersecurity incident at Bausch Health Companies Inc. ("Bausch Health") that involved your personal information. Bausch Health takes data security very seriously, and we sincerely regret that this incident occurred. Although we have no reason to believe that your information has been or will be misused, this letter contains information about what happened, actions we have taken to prevent a reoccurrence, and steps you can take to protect your information.

What Happened?
On July 1, 2026, we identified evidence of unauthorized access to a limited number of company records. We immediately commenced an investigation, which included engaging third-party incident response experts to assist in determining the extent of any unauthorized activity. We have no reason to believe the unauthorized individual continues to have access. Our investigation identified June 24, 2026-July 1, 2026, as the period of unauthorized access.

What Information Was Involved?
After a comprehensive review of the data, we identified on October 28, 2026, that the incident resulted in the acquisition of your name and contact information along with your <<VARIABLE 2>>.

400 Somerset Corporate Boulevard
Bridgewater, New Jersey 08807

908 927 1400
Bauschhealth.com

What We Are Doing
Bausch Health is cooperating fully with law enforcement in relation to this incident. We take the security of all information in our systems very seriously, and we want to assure you that we've launched an investigation with the support of cybersecurity experts. We have hardened our security systems, increased company awareness of data security protection, and will evaluate further technical safeguards. We are also reporting this matter to appropriate privacy regulators and will cooperate with their inquiries.

What You Can Do
We encourage you to remain vigilant for potential fraud or identity theft by reviewing your financial account statements and credit reports for suspicious activity and promptly reporting any concerns. For more resources and information on how to protect yourself, visit the Federal Trade Commission's website on identity theft protection at https://www.identitytheft.gov/.

Additionally, 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 **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. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you believe you are a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

How Do I Enroll For The Free Services?
To enroll in complimentary Credit Monitoring services, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services: <<UNIQUE CODE>>. 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.

Need Assistance?
We are committed to supporting you through this process. If you need assistance, please contact our support team with any questions at **866-746-5463**.

Protecting your information is important to us. We appreciate your patience and understanding.

Sincerely,

Bausch Health Companies Inc.

Additional Important Information

Monitoring: You should always remain vigilant for incidents of fraud and identity theft, especially during the next 12-24 months, by reviewing financial account statements and monitoring your credit reports for suspicious or unusual activity and immediately report any suspicious activity or incidents of identity theft. You have the right to obtain or file a police report. You can contact the Federal Trade Commission (FTC) for more information on preventing identity theft. We encourage you to report any incidents of identity theft to the FTC.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.identitytheft.gov

Credit Reports: You may obtain a copy of your credit report, for free, whether or not you suspect any unauthorized activity on your account, from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You have the right to place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (www.experian.com/fraud/center.html) or Transunion (www.transunion.com/fraud-victim-resource/place-fraud-alert). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency by visiting their websites below or by mail. To place the security freeze for yourself, your spouse, or a minor under the age of 16, you will need to provide your name, address for the past two years, date of birth, Social Security number, proof of identity and proof of address as requested by the credit reporting company. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password, which will be needed to lift the freeze, which you can do either temporarily or permanently. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788 Atlanta, GA 30348-5788 www.equifax.com/personal/credit-report-services/credit-freeze/ 1-866-478-0027	P.O. Box 9554 Allen, TX 75013-9544 http://www.experian.com/freeze/center.html 1-888-397-3742	P.O. Box 160 Woodlyn, PA 19094 www.transunion.com/credit-freeze 1-800-916-8800

For residents of Iowa and Oregon: You are advised to report any suspected identity theft to law enforcement or to the state Attorney General and Federal Trade Commission.

For residents of *New Mexico:* You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident. You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or see the contact information for the Federal Trade Commission.

For residents of District of Columbia, Maryland, New York, North Carolina, and Rhode Island: You can obtain information from the District of Columbia, Maryland, North Carolina, New York, and Rhode Island Offices of the Attorney General and the FTC about fraud alerts, security freezes, and steps you can take to prevent identity theft.

District of Columbia Attorney General	**Maryland Office of Attorney General**	**New York Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
400 6th Street NW Washington, DC 20001 1-202-442-9828 www.oag.dc.gov	200 St. Paul Pl Baltimore, MD 21202 1-888-743-0023 https://www.marylandattorneygeneral.gov/	120 Broadway, 3rd Fl New York, NY 10271 1-800-771-7755 www.ag.ny.gov	9001 Mail Service Ctr Raleigh, NC 27699 1-877-566-7226 https://ncdoj.gov/	150 South Main St Providence RI 02903 1-401-274-4400 www.riag.ri.gov There were 119 Rhode Island residents notified in this incident

400 Somerset Corporate Boulevard
Bridgewater, New Jersey 08807

908 927 1400
Bauschhealth.com

November 25, 2026

VIA US MAIL

<<FIRSTNAME>><<MIDDLE NAME>><<LAST NAME>><<SUFFIX>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>,<<STATE>> <<ZIP CODE>>

Re: <<**VARIABLE 1>>**

Dear Customer,

We are writing to inform you of a recent cybersecurity incident at Bausch Health Companies Inc. ("Bausch Health") that involved your personal information. Bausch Health takes data security very seriously, and we sincerely regret that this incident occurred. Although we have no reason to believe that your information has been or will be misused, this letter contains information about what happened, actions we have taken to prevent a reoccurrence, and steps you can take to protect your information.

What Happened?
On July 1, 2026, we identified evidence of unauthorized access to a limited number of company records. We immediately commenced an investigation, which included engaging third-party incident response experts to assist in determining the extent of any unauthorized activity. We have no reason to believe the unauthorized individual continues to have access. Our investigation identified June 24, 2026-July 1, 2026, as the period of unauthorized access.

What Information Was Involved?
After a comprehensive review of the data, we identified on October 28, 2026, that the incident resulted in the acquisition of your name and contact information along with your <<VARIABLE 2 >>.

400 Somerset Corporate Boulevard
Bridgewater, New Jersey 08807

908 927 1400
Bauschhealth.com

What We Are Doing
Bausch Health is cooperating fully with law enforcement in relation to this incident. We take the security of all information in our systems very seriously, and we want to assure you that we've launched an investigation with the support of cybersecurity experts. We have hardened our security systems, increased company awareness of data security protection, and will evaluate further technical safeguards. We are also reporting this matter to appropriate privacy regulators and will cooperate with their inquiries.

What You Can Do
We encourage you to remain vigilant for potential fraud or identity theft by reviewing your financial account statements and credit reports for suspicious activity and promptly reporting any concerns.

For more resources and information on how to protect yourself, visit the Federal Trade Commission's website on identity theft protection at https://www.identitytheft.gov/.

Need Assistance?
We are committed to supporting you through this process. If you need assistance, please contact our support team with any questions at **866-746-5463**.

Protecting your information is important to us. We appreciate your patience and understanding.

Sincerely,

Bausch Health Companies Inc.

Additional Important Information

Monitoring: You should always remain vigilant for incidents of fraud and identity theft, especially during the next 12-24 months, by reviewing financial account statements and monitoring your credit reports for suspicious or unusual activity and immediately report any suspicious activity or incidents of identity theft. You have the right to obtain or file a police report. You can contact the Federal Trade Commission (FTC) for more information on preventing identity theft. We encourage you to report any incidents of identity theft to the FTC.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.identitytheft.gov

Credit Reports: You may obtain a copy of your credit report, for free, whether or not you suspect any unauthorized activity on your account, from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You have the right to place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (www.experian.com/fraud/center.html) or Transunion (www.transunion.com/fraud-victim-resource/place-fraud-alert). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency by visiting their websites below or by mail. To place the security freeze for yourself, your spouse, or a minor under the age of 16, you will need to provide your name, address for the past two years, date of birth, Social Security number, proof of identity and proof of address as requested by the credit reporting company. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password, which will be needed to lift the freeze, which you can do either temporarily or permanently. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788 Atlanta, GA 30348-5788 www.equifax.com/personal/credit-report-services/credit-freeze/ 1-866-478-0027	P.O. Box 9554 Allen, TX 75013-9544 http://www.experian.com/freeze/center.html 1-888-397-3742	P.O. Box 160 Woodlyn, PA 19094 www.transunion.com/credit-freeze 1-800-916-8800

For residents of Iowa and Oregon: You are advised to report any suspected identity theft to law enforcement or to the state Attorney General and Federal Trade Commission.

For residents of *New Mexico:* You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident. You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or see the contact information for the Federal Trade Commission.

For residents of District of Columbia, Maryland, New York, North Carolina, and Rhode Island: You can obtain information from the District of Columbia, Maryland, North Carolina, New York, and Rhode Island Offices of the Attorney General and the FTC about fraud alerts, security freezes, and steps you can take to prevent identity theft.

District of Columbia Attorney General	**Maryland Office of Attorney General**	**New York Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
400 6th Street NW Washington, DC 20001 1-202-442-9828 www.oag.dc.gov	200 St. Paul Pl Baltimore, MD 21202 1-888-743-0023 https://www.marylandattorneygeneral.gov/	120 Broadway, 3rd Fl New York, NY 10271 1-800-771-7755 www.ag.ny.gov	9001 Mail Service Ctr Raleigh, NC 27699 1-877-566-7226 https://ncdoj.gov/	150 South Main St Providence RI 02903 1-401-274-4400 www.riag.ri.gov There were 119 Rhode Island residents notified in this incident