



[Date]

From:

BioMarin Pharmaceutical Inc.
105 Digital Drive
Novato, CA 94949

To:

[Name]
[Street Address]
[City, State, Zip Code]

***RE: Important Data Privacy Notification
Please read this entire letter.***

Dear [Name]:

We are contacting you regarding a data security incident (the "Incident") involving a "phishing" attack at BioMarin Pharmaceutical Inc. ("BioMarin," the "Company," "we" or "us"). We discovered the Incident on June 21, 2018 and, as described below, have worked diligently to determine the nature and scope of the Incident and its impact. The Incident may have exposed your personal information, including your Social Security Number and health insurance policy number. Please be assured that we are taking steps to address the Incident and to reduce the risk of similar incidents happening in the future.

What happened:

On June 21, 2018, we discovered that someone (the "attacker") had accessed two BioMarin email mailboxes, beginning on June 18, 2018, as a result of a successful phishing attack by which the attacker acquired a temporary employee's user ID and password. When we discovered the breach on June 21, we had the temporary employee change his credentials, thereby preventing further access to the mailboxes. We have so far been unable to determine for certain whether the attacker extracted any or all of the information in the mailboxes before this access was terminated, but it is possible.

Since discovering the Incident, we have been working to secure our network, prevent further attacks, and assess the nature and scope of any personally identifiable information contained in the mailboxes. We recently discovered that a document containing your name and Social Security Number, and another document containing your name and health insurance policy number, may have been in at least one of the mailboxes when they were accessed.

Your Social Security Number:

Because your Social Security Number may have been accessed, we recommend that you place a fraud alert on your credit files. A fraud alert requires potential creditors to use what the law refers to as "reasonable policies and procedures" to verify your identity before issuing credit in your name. A fraud alert lasts for 90 days. By calling one of the three credit reporting agencies listed below, you can automatically place an alert with all of the agencies. You will receive letters from all three, confirming the fraud alert and letting you know how to get a free copy of your credit report from each.

To: [Name]
Date: [Date]
Re: Important Data Privacy Notification
Page 2 of 3

Experian: 1-888-397-3742 P.O. Box 9530 Allen, TX 75013	Equifax: 1-800-525-6285 P.O. Box 740241 Atlanta, GA 30374	TransUnion: 1-800-680-7289 P.O. Box 6790 Fullerton, CA 92834
--	---	--

When you receive your credit reports, look them over carefully. Look for accounts you did not open, inquiries from creditors that you did not initiate, and personal information, such as home address and Social Security Number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a police report of identity theft. Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, we recommend that you check your credit reports periodically. You can keep the fraud alert in place by calling again after 90 days. For more information on identity theft, we suggest that you visit the "Privacy Enforcement and Protection" page on the California Attorney General's website (www.oag.ca.gov/privacy).

Your health insurance policy number:

Because your health insurance policy number may have been accessed, we recommend that you regularly review the explanation of benefits statement that you receive from your plan/insurer. If you see any service that you believe you did not receive, please contact your plan/insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider or plan and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. You can order your reports from the three credit reporting agencies listed above.

Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider/plan, to serve as a baseline.

For more information on identity theft, we suggest that you visit the "Privacy Enforcement and Protection" page on the California Attorney General's website (www.oag.ca.gov/privacy).

To: [Name]
Date: [Date]
Re: Important Data Privacy Notification
Page 3 of 3

What we are doing to protect your information:

To help protect your identity, we are offering a complimentary one-year membership of LifeLock's identity theft protection / credit monitoring. To set up your membership, please follow the instructions below.

To get protection immediately at no cost to you:

1. Call 1-800-899-0180 or visit www.lifelock.com to enroll.
2. Use the promotion code: [Promotion Code] when prompted as well as your Member ID.
3. Your Member ID is [Member ID]

LifeLock's specialized team of telephone representatives is available 24 hours a day, seven days a week to help you enroll in LifeLock.

You will have until December 20, 2018 to enroll in this service.

Once you have completed the LifeLock enrollment process, the services will be in effect immediately. Your LifeLock Standard™ membership includes:

- ✓ LifeLock Identity Alert® System[†]
- ✓ LifeLock Privacy Monitor
- ✓ Live, U.S.-based Member Service Support
- ✓ Identity Restoration Support
- ✓ Priority Live Member Service Support
- ✓ Dollar for Dollar Stolen Funds Reimbursement up to \$25,000 for LifeLock Standard™[‡]

LifeLock backs up its services with its \$1 Million Service Guarantee[‡].

Conclusion:

BioMarin sincerely apologizes for this Incident and regrets any inconvenience it may cause you. Should you have questions or concerns regarding this matter, please do not hesitate to contact [Contact Name] ([Contact Title]) at [Phone Number].

Sincerely,

[Signatory]
[Signatory Title]

No one can prevent all identity theft.

[†] LifeLock does not monitor all transactions at all businesses.

[‡] Stolen Funds Reimbursement benefits and Service Guarantee benefits for State of New York members are provided under a Master Insurance Policy underwritten by State National Insurance Company. Benefits for all other members are provided under a Master Insurance Policy underwritten by United Specialty Insurance Company. Under the Stolen Funds Reimbursement, LifeLock will reimburse stolen funds up to \$25,000 for Standard membership, up to \$100,000 for Advantage membership and up to \$1 million for Ultimate Plus membership. Under the Service Guarantee LifeLock will spend up to \$1 million to hire experts to help your recovery. Please see the policy for terms, conditions and exclusions at LifeLock.com/legal.