Cynthia J. Larose
617 348 1732
cjlarose@mintz.com
mintz.com

MINTZ

One Financial Center
Boston, MA 02111
617 542 6000
617 542 2241 fax

September 21, 2018

Via Email (attorneygeneral@doj.nh.gov) and Federal Express

The Honorable Gordon MacDonald
Attorney General of the State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

RE: Reporting of Security Incident Pursuant to N.H. Rev. Stat. § 359-C:20

Dear Attorney General MacDonald:

This law firm represents BeiGene, Ltd. and its subsidiaries ("BeiGene"), located at 55 Cambridge Parkway, Suite 700W, Cambridge, Massachusetts 02142. Pursuant to New Hampshire Rev. Stat.§ 359-C:20(I)(b), I am writing to notify you of a data security incident that may have resulted in the unauthorized access to personal information involving two (2) residents of New Hampshire. Notice of this incident was mailed to these individuals on September 21, 2018.

In early June, the BeiGene IT team detected suspicious activity in the company's cloud-based email accounts. Upon further review, it was determined that the email accounts of seven BeiGene employees had been accessed in a sophisticated phishing attack. BeiGene promptly took measures to contain the unauthorized access, began an extended investigation into the matter, and has worked diligently to determine what information the attackers potentially viewed and who was potentially impacted. This included hiring a leading cybersecurity forensics firm to support its investigation and validate its remediation efforts, as well as working to obtain log files generated by BeiGene's email provider for the data files at issue.

As BeiGene's investigation continued, it was discovered on August 22, 2018 that from May 22, 2018 until June 8, 2018 the attackers could have viewed certain files containing personal information for employees and former employees. Depending on the circumstances relating to each individual (and as specifically identified in each notice letter), the following personal information may have been accessed: full name, postal address, email address, date of birth, Social Security number, financial account information, credit card information, and copies of documents submitted with an I-9 form to establish identity and employment authorization.

To date, BeiGene has no evidence that any of the personal information was actually accessed or used. BeiGene has arranged to have AllClear ID provide credit monitoring and identity repair services for two years at no cost to the affected individuals. The form of notice to the affected individuals describing the services is attached. BeiGene also notified law enforcement of the incident.

To help prevent a similar incident from occurring in the future, BeiGene is providing additional extensive training to its employees regarding phishing emails and other cybersecurity issues. In addition, BeiGene has enhanced existing measures by implementing multi-factor authentication for email.

MINTZ

If you have any questions or concerns, please do not hesitate to contact me at (617) 348-1732 or at CJLarose@mintz.com.

Very truly yours,

Cynthia J. Larose

Attachments

BeiGene

Processing Center • P.O. BOX 141578 • Austin, TX 78714

SAMPLE #1

00001
R826102

JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

September 21, 2018

NOTICE OF DATA BREACH

Dear JOHN:

We write to inform you of a security incident that that may have affected some of your personal information. Keeping the personal information of our colleagues, as well as others with whom we do business, safe and secure is very important to us, and we regret that this event occurred. We are sending you this letter to provide additional details regarding what happened and to advise you about steps to take in order to help prevent identity theft and fraud.

What Happened

In June, BeiGene's IT team detected suspicious activity in certain of the Company's email accounts. The team immediately commenced an investigation and discovered that the Company had been the victim of a sophisticated email phishing scheme whereby unknown and unauthorized third parties were able to access seven BeiGene email accounts from May 22, 2018 to June 8, 2018. The Company promptly contained the incident and retained independent third-party forensics experts to further investigate. On August 22, 2018, the results of the investigation showed that certain personal information was contained in the email accounts. We have no evidence that any of the personal information was actually accessed or used, but are sending you this notice in an abundance of caution.

What Information Was Involved

Your personal information potentially accessed by the unauthorized parties consisted of the following information: first and last name, home address, Social Security number, and date of birth.

What You Can Do

1. Identity Protection Services. We have retained AllClear ID to protect your identity for the next twenty-four (24) months at no cost to you. The following identity protection services start on the date of this notice and can be used at any time during the next twenty-four (24) months:

BeiGene
Processing Center • P.O. BOX 141578 • Austin, TX 78714

SAMPLE #2

00003
R826102

JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

September 21, 2018

NOTICE OF DATA BREACH

Dear JOHN:

We write to inform you of a security incident that that may have affected some of your personal information. Keeping the personal information of our colleagues, as well as others with whom we do business, safe and secure is very important to us, and we regret that this event occurred. We are sending you this letter to provide additional details regarding what happened and to advise you about steps to take in order to help prevent identity theft and fraud.

What Happened

In June, BeiGene's IT team detected suspicious activity in certain of the Company's email accounts. The team immediately commenced an investigation and discovered that the Company had been the victim of a sophisticated email phishing scheme whereby unknown and unauthorized third parties were able to access seven BeiGene email accounts from May 22, 2018 to June 8, 2018. The Company promptly contained the incident and retained independent third-party forensics experts to further investigate. On August 22, 2018, the results of the investigation showed that certain personal information was contained in the email accounts. We have no evidence that any of the personal information was actually accessed or used, but are sending you this notice in an abundance of caution.

What Information Was Involved

Your personal information potentially accessed by the unauthorized parties consisted of the following information: first and last name, home address, date of birth, and passport number.

What You Can Do

1. Identity Protection Services. We have retained AllClear ID to protect your identity for the next twenty-four (24) months at no cost to you. The following identity protection services start on the date of this notice and can be used at any time during the next twenty-four (24) months:

01-04-3

BeiGene
Processing Center • P.O. BOX 141578 • Austin, TX 78714

SAMPLE #3

00002
R826102
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

September 21, 2018

NOTICE OF DATA BREACH

Dear JOHN:

We write to inform you of a security incident that that may have affected some of your personal information. Keeping the personal information of our colleagues, as well as others with whom we do business, safe and secure is very important to us, and we regret that this event occurred. We are sending you this letter to provide additional details regarding what happened and to advise you about steps to take in order to help prevent identity theft and fraud.

What Happened

In June, BeiGene's IT team detected suspicious activity in certain of the Company's email accounts. The team immediately commenced an investigation and discovered that the Company had been the victim of a sophisticated email phishing scheme whereby unknown and unauthorized third parties were able to access seven BeiGene email accounts from May 22, 2018 to June 8, 2018. The Company promptly contained the incident and retained independent third-party forensics experts to further investigate. On August 22, 2018, the results of the investigation showed that certain personal information was contained in the email accounts. We have no evidence that any of the personal information was actually accessed or used, but are sending you this notice in an abundance of caution.

What Information Was Involved

Your personal information potentially accessed by the unauthorized parties consisted of the following information: first and last name, home address, and Social Security number.

What You Can Do

1. Identity Protection Services. We have retained AllClear ID to protect your identity for the next twenty-four (24) months at no cost to you. The following identity protection services start on the date of this notice and can be used at any time during the next twenty-four (24) months:

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-471-8393 and a dedicated investigator will help recover financial losses, restore your credit, and make sure your identity is returned to its proper condition. Detailed information regarding the AllClear Identity Repair service (Terms of Use) is included with this letter.

AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a $1 million identity theft insurance policy. To enroll in this service, you will need to provide your personal information to AllClear ID. You may enroll online at enroll.allclearid.com or by phone by calling 1-855-471-8393 using the following redemption code: Redemption Code.

Please note: Following enrollment, additional steps are required to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may also be required to activate your monitoring options.

2. Fraud Alert. If you do not choose to activate the AllClear ID identity protection services, we recommend that you place a fraud alert on your credit file. A fraud alert requires potential creditors to verify your identity before issuing credit in your name. A fraud alert lasts for ninety days or until you choose to remove if earlier. Please note that no one is allowed to place a fraud alert on your credit report except for you. All you need to do is contact one of the three credit reporting agencies by using the contact details provided below. Doing so will automatically place an alert with all three agencies. You will receive letters from each confirming the fraud alert and letting you know how to get a free copy of your credit report.

- **Experian**
  - Phone: 1-888-397-3742 (US toll-free number)
  - Address: P.O. Box 4500, Allen, TX 75013
  - Online: www.experian.com

- **TransUnion**
  - Phone: 1-800-680-7289 (US toll-free number)
  - Address: P.O. Box 2000, Chester, PA 19022
  - Online: www.transunion.com

- **Equifax**
  - Phone: 1-800-525-6285 (US toll-free number)
  - Address: P.O. Box 740241, Atlanta, GA 30374
  - Online: www.equifax.com

3. Credit Freezes.

Credit freeze information for Massachusetts residents: Massachusetts law gives you the right to place a security (credit) freeze on your credit reports. A security (credit) freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security (credit) freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit reports by sending a request to the credit reporting agencies listed above by certified mail, overnight mail or regular mail. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company at the addresses above.* The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law

enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). Federal law prohibits credit reporting companies from charging fees for credit freezes.

Credit freeze information for Rhode Island residents: Rhode Island law gives you the right to place a security (credit) freeze on your credit reports. A security (credit) freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security (credit) freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address listed above. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company at the addresses above.* The following information should be included when requesting a security freeze: full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or valid police report, investigative report, or compliant with a law enforcement agency about the unlawful use of your identifying information. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). Federal law prohibits credit reporting companies from charging fees for credit freezes.

Credit freeze information for residents of states other than Massachusetts and Rhode Island: In addition to the AllClear ID services (or the fraud alert), a credit freeze is a further step to help alleviate concerns about becoming a victim of identity theft or fraud. It prevents creditors from seeing your credit report and credit score unless you decide to unlock the credit reporting file using a PIN code. Please note that when you have a credit freeze in place, you will be required to take special steps in order to apply for any type of credit. Federal law prohibits credit reporting companies from charging fees for credit freezes. *Unlike a fraud alert, each credit reporting agency must be contacted individually.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies by using these contact details:

- **Experian** Address: P.O. Box 9554, Allen, TX 75013
- Online: www.experian.com

- **TransUnion** Address: P.O. Box 2000, Chester, PA 19022
- Online: www.transunion.com

- **Equifax** Address: P.O. Box 105788, Atlanta, GA 30348
- Online: www.equifax.com

4. Keep Aware! It is essential that you remain vigilant for incidents of identity theft and fraud. You should frequently review account statements and monitor your free credit reports. Look for accounts you did not open or inquiries from creditors that you did not initiate. If you see anything suspicious, immediately call the credit reporting agency at the telephone number on the report and report the suspicious activity to AllClear ID as described elsewhere in this letter. It is also advisable to report suspected identity theft to local police and to the Attorney General's office in your state.

What We Are Doing

BeiGene is aware of the increasing threat of cybersecurity attacks and we are committed to making sure that we have enhanced security measures in place and effective training for our employees in order to help prevent such attacks from happening. We will continue to work hard in this regard and remain confident in our ability to protect your personal information.

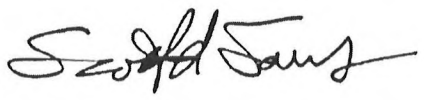
For More Information

Please refer to the Appendix to this notice for additional information about protecting your identity or about how to respond if you are the victim of identity theft. For US residents, information relevant to the state where you reside may also be found on the Appendix.

If you have further questions or concerns about this incident, you may contact our dedicated assistance line at 1-855-471-8393, Monday through Saturday, 9 a.m. through 9 p.m. ET.

Please accept our sincerest apologies for any inconvenience caused by this incident.

Very truly yours,



Scott A. Samuels
Senior Vice President, General Counsel
BeiGene, Ltd.

APPENDIX

Information about Identity Theft Prevention

If you are the victim of identity theft, we encourage you to contact local law enforcement, the Attorney General's office in your state, and the Federal Trade Commission (contact details below). From these government agencies you can also obtain additional information about fraud alerts and credit freezes and learn more about preventing and managing identity theft and fraud.

Federal Trade Commission
877-438-4338 (toll-free number)
www.identitytheft.gov/
600 Pennsylvania Ave., NW
Washington, DC 20580

To file a complaint with the FTC, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338) (toll-free number). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

Residents of Massachusetts: You have the right to obtain a police report.

Residents of North Carolina: You may obtain information about preventing and avoiding identity theft from the Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM (toll-free number), www.ncdoj.gov.

Residents of Rhode Island: You also have the right to file or obtain a police report, and you may obtain information about preventing and avoiding identity theft from the Rhode Island Attorney General's Office:

Rhode Island Attorney General's Office, Consumer Protection Unit
150 South Main Street, Providence, RI 02903, 401-274-4400, http://www.riag.ri.gov/

AllClear Identity Repair Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 24 months of coverage with no enrollment required.
- No cost to you — ever. AllClear Identity Repair is paid for by the participating Company.

Services Provided
If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Identity Repair is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period
Service is automatically available to you with no enrollment required for 24 months from the date of the breach incident notification you received from Company (the "Coverage Period"). Fraud Events (each, an "Event") that were discovered prior to your Coverage Period are not covered by AllClear Identity Repair services.

Eligibility Requirements
To be eligible for Services under AllClear Identity Repair coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim
If you become a victim of fraud covered by the AllClear Identity Repair services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Identity Repair by providing the redemption code on the notification letter you received from the sponsor Company;
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

Coverage under AllClear Identity Repair Does Not Apply to the Following:
Any expense, damage or loss:

- Due to
  - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge, or
  - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation");
- Incurred by you from an Event that did not occur during your coverage period; or
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Identity Repair coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity.
- AllClear ID is not an insurance company, and AllClear Identity Repair is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of AllClear Identity Repair coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy
If for any reason you wish to have your information removed from the eligibility database for AllClear Identity Repair, please contact AllClear ID:

E-mail	Mail	Phone
support@allclearid.com	AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	1.855.434.8077

package id
0315158
ship date
Thu, Sep 20 2018
to
Hon. Gordon MacDonald
Office of the Attorney General - NH
33 CAPITOL ST
CONCORD, NH 03301-6310
United States
617-348-1732
residential address
No
return label
No

from
Cynthia J Larose (CJLarose)
Mintz Levin
One Financial Center
Boston, MA 02111
US
16173481732
billing
BEIGENE LTD..Data Security Matter (041891.013)
operator
Susan Manning
617-210-6812
smanning@mintz.com
create time
09/20/18, 11:21AM

vendor
FedEx
tracking number
782859850499
service
FedEx Priority Overnight®
packaging
FedEx® Envelope
signature
Direct Signature Required
courtesy quote
14.27

Quote may not reflect all accessorial charges