

2016 JUN -1 AM 10: 24

May 31, 2016

*Via Email ([attorneygeneral@doj.nh.gov](mailto:attorneygeneral@doj.nh.gov)) and Federal Express*

The Honorable Joseph Foster  
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. Section 359-C:20

Dear Attorney General Foster:

This law firm represents ARIAD Pharmaceuticals, Inc. (the "Company"). On March 31, 2016, an unknown, unauthorized person from outside the Company impersonated a member of the Company's leadership team and, using what appeared to be that person's legitimate Company email address, convinced an employee of the Company to provide certain personal information about current and former employees. The possibility of inadvertent disclosure was brought to the attention of the Company's legal counsel on May 4, 2016, and an investigation began immediately to determine what happened and to resolve this unfortunate situation. This letter serves to notify your office of the situation, and to comply with the requirements of N.H. Rev. Stat. Section 359-C:20.

### *Nature of the Security Incident*

The disclosure that occurred was the result of human error prompted by a sophisticated phishing scam. The incident did not involve any customer information or an intrusion into ARIAD's computer systems or network.

We are also actively investigating a potential security incident with ARIAD's provider, ADP. We have learned that a number of companies utilizing ADP's external payroll and W-2 portal (as does ARIAD) have discovered unauthorized access to that portal through a technical weakness in the ADP system that was publicly reported in early May. We have changed the way ARIAD access to the ADP portal is provided, and are working with ADP on the investigation.

### *Nature of the Information Acquired and Number of Affected New Hampshire Residents*

The personal information disclosed to the unknown third person consisted of the following information for each individual affected: first and last name, home address, Social Security number, salary information, deductions and other information disclosed on their W-2 tax form. Our analysis suggests that the aforementioned personal information of five (5) New Hampshire residents was disclosed to the unauthorized third party.

**Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C.**

Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C.

The Honorable Joseph Foster  
Attorney General of the State of New Hampshire  
May 31, 2016  
Page 2

*Remediation Steps*

The Company will be providing notice to all affected individuals, including both current and former employees, and will be providing five (5) years of identity protection and credit monitoring services through AllClear ID at no cost to any of the individuals affected. Additionally, the Company is continuing to assess its procedures and employee training and awareness programs to ensure that personal information is protected.

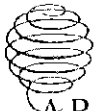
A sample copy of the Company's notification to the affected New Hampshire residents is attached. The notification will be mailed to affected residents no later than June 1, 2016.

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

Very truly yours,

A handwritten signature in black ink, appearing to read "Cynthia J. Larose". The signature is fluid and cursive, with the first name "Cynthia" and last name "Larose" clearly distinguishable.

Cynthia J. Larose



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



00001  
JOHN Q. SAMPLE  
1234 MAIN STREET  
ANYTOWN US 12345-6789

June 1, 2016

## NOTICE OF DATA BREACH

Dear John:

We are writing to you because of a recent “phishing” scam that has resulted in an inadvertent disclosure of your personal information. We deeply regret that this has occurred and are sending you this letter to provide additional details regarding what happened and to advise you about steps to take to help prevent identity theft and fraud.

### What Happened

On March 31, 2016, an unknown, unauthorized person from outside of ARIAD impersonated a member of ARIAD’s executive leadership team and, using what appeared to be that person’s legitimate ARIAD email address, convinced one of our employees to provide certain personal information about current and former personnel. The possibility of inadvertent disclosure was brought to the attention of ARIAD’s legal counsel on May 4, 2016, and an investigation began immediately to determine what happened. This information was stolen through a sophisticated phishing scam for employee information, much like the phishing scams you may have read about in the news that have affected many companies and tens of thousands of individuals. It did not involve any intrusion into our computer systems or network -- this disclosure was the result of an unfortunate human error, not a failure of network security.

We are also actively investigating a potential security incident with ARIAD’s provider, ADP. We have learned that a number of companies utilizing ADP’s external payroll and W-2 portal (as does ARIAD) have discovered unauthorized access to that portal through a technical weakness in the ADP system. We have changed the way ARIAD access to the ADP portal is provided, and are working with ADP on the investigation.

### What Information Was Involved

The personal information disclosed to the unknown third person consisted of the following information for each individual affected: first and last name, home address, Social Security number, salary information, deductions and other information disclosed on your W-2 tax form. The disclosure did not include any bank or financial account information (such as a routing number), spousal or dependent information or health information.

### What You Can Do

We recommend that you take these immediate next steps:

1. **IRS Notices.** You should complete Form 14039-Identity Theft Affidavit (<https://www.irs.gov/pub/irs-pdf/f14039.pdf>) and submit this form to the Internal Revenue Service (“IRS”) by fax or mail. This is a proactive measure to notify the IRS that your personal information may have been compromised and to alert them about potential suspicious activity involving your tax return. The IRS has published informational “tips” at: <https://www.irs.gov/uac/Newsroom/Tips-for-Taxpayers.-Victims-about-Identity-Theft-and-Tax>Returns>. You should also check your state tax authority’s website to determine whether the state has a similar identity theft affidavit. You should file these affidavits even if you have already filed your 2015 tax returns.



01-03-1-00

2. **Identity Protection Services.** To ensure that we are taking proactive steps to protect you against identity theft or fraud, we have arranged to have AllClear ID protect your identity for the next 60 months at no cost to you. The following identity protection services start on the date of this notice:

- AllClear SECURE: This is an “identity repair” service. You are automatically eligible to use this service and no enrollment is required. If a problem arises, simply call 1-855-285-8914 and a dedicated investigator will help you recover financial losses, restore your credit and make sure your identity is returned to its proper condition.
- AllClear PRO: This service offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. To use the PRO service, you will need to provide your personal information to AllClear ID. You may sign up online at [enroll.allclearid.com](http://enroll.allclearid.com) or by phone at 1-855-285-8914 using the following redemption code: Redemption Code.

Information on the services and how to take advantage of them is described in the AllClear Terms of Use attached as Appendix B to this letter. Please note that additional steps may be required by you to activate your phone alerts and monitoring options.

3. **Fraud Alert.** Because your Social Security number was involved, 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 it at an earlier time. Please note that no one is allowed to place a fraud alert on your credit report except for you. If you contact one of the three credit reporting agencies below, you 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 (toll-free number)
  - Address: P.O. Box 4500, Allen, TX 75013
  - Online: [www.experian.com](http://www.experian.com)
- **TransUnion**
  - Phone: 1-800-680-7289 (toll-free number)
  - Address: P.O. Box 2000, Chester, PA 19022
  - Online: [www.transunion.com](http://www.transunion.com)
- **Equifax**
  - Phone: 1-800-525-6285 (toll-free number)
  - Address: P.O. Box 740241, Atlanta, GA 30374
  - Online: [www.equifax.com](http://www.equifax.com)

4. **Credit Freezes (for non-Massachusetts residents).** 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. Credit freeze laws vary from state to state and the cost of placing, temporarily lifting, and removing a credit freeze varies by state (generally \$5 to \$20 per action at each credit reporting agency). *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](http://www.experian.com)

- o **TransUnion** Address: P.O. Box 2000, Chester, PA 19022
- o Online: [www.transunion.com](http://www.transunion.com)
  
- o **Equifax** Address: P.O. Box 105788, Atlanta, GA 30348
- o Online: [www.equifax.com](http://www.equifax.com)

5. 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.* 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). The credit reporting company may charge a reasonable fee of up to \$5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft and have submitted a valid police report relating to the identity theft to the credit reporting company.

6. Be 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**

ARIAD is aware of the increasing threat of cybersecurity attacks and we are committed to ensuring that we have security measures in place and effective training for our employees to help prevent such attacks from happening.

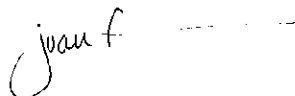
**For More Information**

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

This notice is dated June 1, 2016 and is provided by ARIAD Pharmaceuticals, Inc., 26 Landsdowne Street, Cambridge, Massachusetts 02139-4234.

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

Very truly yours,



Joan Meissner  
 Assistant General Counsel, Sr. Director,  
 Compliance



## **APPENDIX A**

### **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/](http://www.identitytheft.gov/)  
600 Pennsylvania Ave., NW  
Washington, DC 20580

To file a complaint with the FTC, go to [www.ftc.gov/idtheft](http://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.

**For residents of Maryland:** You may obtain information about preventing and avoiding identity theft from the Attorney General:

**Maryland Office of the Attorney General**, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 (toll-free number), [www.oag.state.md](http://www.oag.state.md).

**For residents of Massachusetts:** You have the right to obtain a police report.

**For 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](http://www.ncdoj.gov).

## **APPENDIX B**

### **AllClear Secure 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:

- 60 months of coverage with no enrollment required;
- No cost to you – ever. AllClear Secure 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 Secure 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 60 months from the date of the breach incident notification you received from Company (the “Coverage Period”). Fraud events that occurred prior to your Coverage Period are not covered by AllClear Secure services.

#### **Eligibility Requirements**

To be eligible for Services under AllClear Secure 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 Secure services (an “Event”), 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 Secure 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 Secure 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 Secure 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 Secure 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 Secure 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 Secure, please contact AllClear ID:

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