

2016 APR 21 AM 9:52

April 19, 2016

VIA FED-EX

Attorney General Joseph Foster
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Dear Attorney General Foster:

I am writing to notify your office that Agenus recently confirmed that certain personally identifiable information ("PII") retained by Agenus in the course of its business operations may have been compromised as part of a spear phishing incident. An unknown entity used a spear phishing technique to obtain personal information about Agenus' employees by inducing one employee to send certain employee W-2 forms to the entity under false pretense. Agenus first discovered the incident on April 18, 2016, which is the same day that the W-2 forms were sent out under false pretense. Since then, Agenus has been investigating the incident. In addition to Agenus' own investigation, this incident has been reported to law enforcement authorities. Agenus is fully cooperating with law enforcement in investigating and responding to the incident.

Although the investigation is ongoing, at this point we have determined that 5 residents of your state may have been affected, and we believe that the information compromised may have included names, addresses, Social Security numbers, and salary information. However, due to the ongoing nature of this investigation, this number is subject to change, and we will continue to update your office if we identify additional residents who may have been affected.

Letters substantially similar to the enclosed consumer notification letter were sent on April 19, 2016 to the residents in your state whose PII may have been compromised. In addition, as reflected in the notification letter, we have arranged for AllClear ID to provide identity theft protection to all individuals whose PII may have been compromised at no charge to them. We have also recommended measures that affected individuals should consider taking (at Agenus' cost) to further guard against the potential misuse of their personal information, including the option to place a security freeze on their credit files.

If you have any questions, please do not hesitate to contact Karen Valentine, Chief Legal Office & General Counsel at 781-674-4678 or karen.valentine@agenusbio.com.

Sincerely,



Christine M. Klaskin
VP, Finance

Enclosure: *Form of Consumer Notification Letter*

I am writing to inform you that on April 18, 2016 your personal data was mistakenly released to a third party in response to a fraudulent inquiry. Information revealed included your W-2 form, which included your name, address, social security number and salary information for 2015. The W-2 form did not include your bank account information. We have notified authorities and secured a service provider (AllClear ID) with expertise in mitigating the personal risk to you. Management will make it a highest priority to assist you in minimizing your financial exposure and any inconvenience. Attached is a summary of the procedures and resources available, including information on AllClear ID and the services they will provide to you free of charge for the next two years. We are also offering 1:1 assistance with a member of finance or human resources to assist you directly in this process. We will conduct a brief overview tomorrow morning at 10am (invitation to follow), and you may sign up for assistance at that time. You may also contact [xxxxxxx] directly at [xxxxxxx] if you have any questions in the meantime.

If you prefer to take immediate action yourself, please refer to the resources and steps outlined in the attachment, which include information on monitoring free credit reports, information for the major credit reporting agencies, information on how to place a credit freeze, and detailed information from AllClear ID on the services they will provide to you free of charge for the next two years. Please note that AllClear ID offers varying levels of services, some of which will require you to use the redemption code provided that is personalized to you.

Please know that we have policies in place to protect your personal information, took immediate steps to address the source of this incident, and are committed to preventing any future exposures.

Dear

We have arranged to have AllClear ID protect your identity for two (2) years at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next two (2) years.

The team at AllClear ID is ready and standing by if you need identity repair assistance. This service is automatically available to you with no enrollment required. If a problem arises, simply call 877-676-0379 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

The company is also providing AllClear PRO, AllClear ID's highest level of service: 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 using your personalized redemption code (xxxxxxx).

Terms of Use:

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 two (2) years 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, 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;
- 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
 - 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;
- 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; and
- 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:

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

Additional Information about Identity Theft Prevention

Below is a list of various steps that you can take to further guard against potential misuse of your personal information, including the option to place a security freeze on your credit file.

If you find suspicious activity on your credit reports or account statements, or have reason to believe that your personal information is being misused, contact your local law enforcement authorities immediately and file a police report. You have the right to request a copy of the police report and should retain it for further use, as many creditors want the information it contains to absolve you of potential fraudulent

debts. In addition, the IRS provides additional guidance regarding tax-related identity theft, available at <https://www.irs.gov/Individuals/Identity-Protection>.

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax: P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
Experian: P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion: P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for 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.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

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

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

Maryland Office of the Attorney General, Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

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

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina 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, www.ncdoj.gov

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-888-766-0008, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, fraud.transunion.com

Credit Freezes (for Non-Massachusetts Residents): You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the

use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Credit Freezes (for Massachusetts Residents): Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security 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 below:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

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.