

Joshua A. James
Direct: (202) 508-6265
josh.james@bryancave.com

March 13, 2017

CONFIDENTIAL

VIA FEDERAL EXPRESS

State of New Hampshire Department of Justice
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Data Security Breach Notification

To Whom It May Concern:

In compliance with N.H. Rev. Stat. 359-C:19, Biomedical Systems Corp. ("Biomedical"), a client of Bryan Cave LLP, is notifying the New Hampshire Department of Justice that Biomedical is notifying 1 individual who resides in New Hampshire of a W-2 phishing attack that affected the personal information of employees who worked with Biomedical during 2016.

This incident occurred on Thursday, March 2, 2017. Most current employees were initially informed of this incident via-email on Friday, March 3, 2017. The attached letter is being mailed to all affected individuals (current and former employees) on March 14, 2017.

Law enforcement and the IRS were contacted by Biomedical on March 2, 2017. Biomedical is providing affected individuals with three years of free credit monitoring and ID restoration services through AllClear ID. Information regarding this service, as well as additional information to assist individuals, is included in the notification sent to the affected individual.

If you would like any additional information concerning the above event, please feel free to contact me at your convenience.

Sincerely,

/s/ Joshua James

Joshua James

Attachment

2017 MAR 13 PM 10:36

STATE OF NH
DEPT OF JUSTICE

ATTACHMENT



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

March 14, 2017

Notice of Data Breach

Dear John Sample,

We have reason to believe that our company has fallen victim to a criminal's attempt to fraudulently obtain our employees' W-2 information. Such attacks are, unfortunately, becoming increasingly common as cyber thieves attempt to obtain employee W-2 information in order to file fraudulent tax returns. Below is additional information about this event, steps you can take to help protect yourself, and efforts we are taking to help protect you.

What Happened?

A criminal posing as a member of Biomedical Systems' management team obtained copies of Biomedical Systems' employees' Form W-2 for 2016.

What Information Was Involved?

Employee W-2 information was involved in this incident. This information includes your name, your Social Security number, your address, your employer's name and address, and your earnings information for 2016 such as wages, withholdings, and taxes. Both current and former employees that receive a 2016 Form W-2 from Biomedical Systems are impacted by this incident.

What You Can Do.

There are several steps that you can take to help reduce your chances of tax fraud or identity theft related to this incident.

If you have not already filed your tax return, it is recommended that you promptly file the Form 14039 Affidavit that we provided via email on March 3, 2017. This form is also available at: <https://www.irs.gov/pub/irs-pdf/f14039.pdf>.

You may also want to consider placing an initial fraud alert or a credit freeze on your credit reports with the three national credit bureaus. Information about fraud alerts, credit freezes, and general steps you can take to protect yourself from identity theft can be found below under the heading "Information about Identity Protection."

What We Are Doing.

We have notified the IRS and law enforcement of this incident (including the FBI) and have indicated our willingness to cooperate concerning impacted employees.

As an added precaution, we have arranged to have AllClear ID protect your identity for 36 months 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 36 months.

AllClear Identity Repair: 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 1-855-836-9840 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

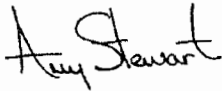


AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-836-9840 using the following redemption code: Redemption Code.

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

We sincerely regret that this situation occurred and apologize for any inconvenience it may have caused you. If you have any questions about the security incident or the protection services please call AllClear ID directly at 1-855-836-9840. If you have any additional questions please contact me directly at (314) 576-6800 (BMS extension 3001) or at astewart@biomedsys.com.

Sincerely,

A handwritten signature in cursive script that reads "Amy Stewart". The signature is written in black ink and is positioned above the typed name.

Amy Stewart
Chief Human Resources Officer
Biomedical Systems Corp.

Information about Identity Protection

We recommend you remain vigilant 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").

We recommend that, as a general matter, you 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, 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 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.

Additionally, if you believe that you have been the victim of identity theft, you have the right to file a police report regarding that incident and obtain a copy of that police report. You may also obtain a police report regarding this incident if any is filed.

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, www.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.

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

You can obtain more information about fraud alerts, credit freezes, and identity theft by contacting one of the national credit reporting agencies listed above or the FTC. The FTC may be reached at:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
Tel: 1-877-438-4338
www.identitytheft.gov/

If you are a resident of Maryland or North Carolina, you can obtain additional information for how to avoid identity theft and how to report identity theft from the following sources.

MD Attorney General's Office Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us	NC Attorney General's Office Consumer Protection Division 9001 Mail Service Center Raleigh, NC 27699-9001 1-877-566-7226 http://www.ncdoj.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:

- 36 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 36 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 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;
- 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
 - o Any transactions on your financial accounts made by authorized users, even if acting without your knowledge
 - o 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 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; 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 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 support@allclearid.com	Mail AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	Phone 1.855.434.8077
---	--	--------------------------------

AllClear Credit Monitoring End User Agreement Information:

Whereas everyone that receives this letter automatically has access to AllClear Identity Repair, the AllClear Credit Monitoring service is optional and requires you to sign up. If you decide to sign up for the AllClear Credit Monitoring service, the terms applicable to that service are available at: <https://www.allclearid.com/end-user-services-agreement/>.

