

# BakerHostetler

## Baker & Hostetler LLP

312 Walnut Street  
Suite 3200  
Cincinnati, OH 45202-4074

T 513.929.3400  
F 513.929.0303  
www.bakerlaw.com

Patrick H. Haggerty  
direct dial: 513.929.3412  
phaggerty@bakerlaw.com

June 14, 2016

**VIA OVERNIGHT MAIL AND E-MAIL**  
**(IDTHEFT@OAG.STATE.MD.US)**

Brian E. Frosh  
Attorney General  
Office of the Attorney General  
Attn: Security Breach Notification  
200 St. Paul Place  
Baltimore, MD 21202

*Re: Incident Notification*

Dear Mr. Frosh:

Our client, BioTime, Inc. and its subsidiaries (“**BioTime**”), on June 9, 2016, learned that a targeted “phishing” email message had been sent from outside the company to a BioTime employee that same day. Upon learning this, BioTime immediately began an internal investigation. The investigation revealed that the phishing email the employee received was designed to appear as though it had been sent by a BioTime executive and requested 2015 IRS Forms W-2. Believing the email to be legitimate, the employee replied to the message and attached 2015 W-2s, which included the names, addresses, Social Security numbers, and earnings for current and former BioTime employees who received a 2015 W-2 from BioTime. The FBI, IRS, and state taxing authorities have been notified of this incident and BioTime is cooperating with their investigation.

BioTime provided an email notification of this incident to affected current employees on June 10, 2016, and began mailing notification letters to the home addresses of affected current and former employees on June 14, 2016. BioTime is offering affected current and former employees two years of credit monitoring and identity theft protection services through Experian. BioTime also is providing call center support for those affected.

BioTime is notifying one Maryland resident via U.S. mail in substantially the same form as the letter attached hereto.<sup>1</sup> Notification is being provided in the most expedient time possible and without unreasonable delay pursuant to the investigation described above, which was necessary to determine the scope of the incident and identify the individuals potentially affected. *See* MD. CODE, COM. LAW § 14-3504(d)(1)(ii).

BioTime is aggressively analyzing where process improvements are needed and will implement those changes as quickly as it can to help prevent any similar accident from occurring in the future.

Please do not hesitate to contact me if you any have questions regarding this matter.

Sincerely,



Patrick H. Haggerty  
Partner

Enclosure

---

<sup>1</sup> This report is not, and does not constitute, a waiver of personal jurisdiction.

[BioTime Letterhead]  
[Return Address-BioTime]

[Date]

Recipient Name  
Address  
Address

Dear [Recipient Name]:

BioTime is committed to maintaining the privacy and security of our current and former employees' personal information. Regrettably, we are writing to inform you of an incident involving some of that information.

### **What happened?**

On June 9, 2016, we learned that a targeted "spear phishing" email message had been sent to a BioTime employee that same day. Spear phishing emails are an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques. Phishing emails are crafted to appear as if they have been sent from a legitimate organization or known individual. The email our employee received was designed to appear as though it had been sent to the employee by a BioTime executive, from the BioTime executive's email account, requesting employees' 2015 IRS Form W-2s. Believing the email to be legitimate, the employee responded to the email and attached employees' 2015 IRS Form W-2s, which included your name, address, Social Security number, and earnings information. Since discovering this incident, we have notified the FBI, the IRS and state tax authorities of this incident.

### **What Information Was Involved?**

The information involved in this incident included the names, addresses, Social Security numbers, and earnings information for BioTime employees who were issued a W-2 for the 2015 tax year.

### **What We Are Doing.**

We recognize this issue can be concerning and frustrating and we are taking steps to help protect you and to safeguard the personal information we receive and maintain going forward. We are offering a complimentary two-year membership of Experian's® ProtectMyID® Elite. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft. ProtectMyID Elite is completely free and enrolling in this program will not hurt your credit score. Unfortunately, due to privacy laws, we are not able to enroll you directly. Each employee must enroll themselves personally. For more information on ProtectMyID Elite and instructions on how to activate your complimentary two-year membership, please see below:

#### **ACTIVATE PROTECTMYID NOW IN THREE EASY STEPS:**

1. **ENSURE** that you enroll by: September 30, 2016. Your code will not work after this date.
2. **VISIT** the ProtectMyID Web Site to enroll: [www.protectmyid.com/enroll](http://www.protectmyid.com/enroll)
3. **PROVIDE** your personal Activation Code: [insert code]

If you have questions or need an alternative to enrolling online, please call 877-441-6943 and provide the customer service representative with the engagement number: **PC102086**.

#### **ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN PROTECTMYID MEMBERSHIP:**

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
  - **Daily 3 Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax<sup>®</sup>, and TransUnion<sup>®</sup> credit reports.
  - **Internet Scan:** Alerts if your personal information is located on sites where compromised data is found, traded or sold.
  - **Change of Address:** Alerts of any changes in your mailing address.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
  - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE<sup>™</sup>, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **\$1 Million Identity Theft Insurance<sup>1</sup>:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.
- **Lost Wallet Protection:** If you misplace or have your wallet stolen, an agent will help you cancel your credit, debit, and medical insurance cards.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-441-6943.

#### **What You Can Do.**

Attached is a list of FAQs that provides further information about this incident as well as information regarding additional steps you can take to protect your personal information. We encourage you to review these FAQs, remain vigilant, and to sign up for the Experian services.

Even if you choose not to take advantage of the identity theft protection services we are offering, we recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your credit card, bank, and other financial statements for any unauthorized activity. You may also obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies once every 12 months. To order your credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting agencies is as follows:

#### **Equifax**

P.O. Box 740241  
Atlanta, GA 30374  
[www.equifax.com](http://www.equifax.com)  
(800) 685-1111

#### **Experian**

P.O. Box 2002  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)  
(888) 397-3742

#### **TransUnion**

P.O. Box 2000  
Chester, PA 19016  
[www.transunion.com](http://www.transunion.com)  
(800) 916-8800

---

<sup>1</sup> Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should contact the Federal Trade Commission and/or the Office of the Attorney General in Maryland. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission and the Maryland Attorney General's Office is as follows:

Federal Trade Commission  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)  
(877) 438-4338

Maryland Attorney General's Office  
200 St. Paul Place  
Baltimore, MD 21202  
[www.oag.state.md.us](http://www.oag.state.md.us)  
(888) 743-0023 (toll free when calling within Maryland)  
(410) 576-6300 (for calls originating outside Maryland)

*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](http://www.equifax.com)  
Experian: 1-888-397-3742, [www.experian.com](http://www.experian.com)  
TransUnion: 1-800-680-7289, [fraud.transunion.com](http://fraud.transunion.com)

*Credit Freezes:* 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 Security Freeze: P.O. Box 105788, Atlanta, GA 30348, [www.equifax.com](http://www.equifax.com)  
Experian Security Freeze: P.O. Box 9554, Allen, TX 75013, [www.experian.com](http://www.experian.com)  
TransUnion Security Freeze: P.O. Box 2000, Chester, PA, 19022-2000, [freeze.transunion.com](http://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.

#### **For More Information.**

We deeply regret this incident occurred and we offer our sincerest apologies to everyone affected. We are aggressively analyzing where process improvements are needed and will implement those changes as quickly as we can to help prevent any similar accident from occurring in the future.

Should you have further questions regarding this incident, please contact me at 510-775-0431.

Sincerely,

Tracey Erwin  
Head of Human Resources (contract)