

February 16, 2018

Bialy/Thomas & Associates  
1149 N. Gower St.  
Suite 242  
Los Angeles, CA 90038

<<FirstName>><<LastName>>  
<<Address1>><<Address2>>  
<<City>>, <<State>> <<Zip>>

**Re: NOTICE OF DATA BREACH**

Dear <<FirstName>><<LastName>>,

**[[THIS LETTER WILL BE SENT TO ONE MONTANA RESIDENT]]**

**What Happened**

I am writing to inform you about a data security incident affecting an email account used by an individual working in our business. From what we can tell, an unauthorized person or persons successfully perpetrated a phishing attack and used the compromised account credentials to send a number of suspicious emails on November 16, 2017, at which time we became aware of the compromise and took immediate steps to secure the account. Out of an abundance of caution, the following day we began working with a team of cybersecurity experts to investigate the breadth and depth of the incident. As a result of this investigation, we have learned that the data security incident in question is likely to have occurred on or about August 22, 2017 and that it appears that the affected account contained information about some of the individuals we have worked with, including you.

**What Information Was Involved**

While the investigation continues, our current understanding is that the affected personal information may include your Social Security number, government-issued ID information (such as a driver's license number, passport number, Tax ID number, or Employer Identification Number); and/or online account credentials.

**What We Are Doing**

We take the privacy and security of your personal information very seriously. As soon as we learned of the compromise, we took immediate steps to secure the account and consulted with cybersecurity experts to launch an investigation. In addition, we are

To Enroll, Please Call:  
[xxx-xxx-xxxx]

Or Visit:  
[www.xxxxxxx.com/xxxxx](http://www.xxxxxxx.com/xxxxx)

Enrollment Code:  
[xxxxxxxxxxxxxx]

reviewing and updating our security practices in order to help prevent this type of incident from occurring again.

### **What You Can Do**

As an added precaution, we have arranged to have AllClear ID protect your identity for 24 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 24 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call «DID\_Phone» and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

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. For a child under 18 years old, AllClear ID ChildScan identifies acts of fraud against children by searching thousands of public databases for use of your child's information. To enroll in this 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 by calling «DID\_Phone» using the following redemption code: {RedemptionCode}.

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

Even if you choose not to enroll in the services, we recommend that you remain vigilant and take steps to protect yourself from identity theft by reviewing your account statements and by checking your credit report from one or more of the national credit reporting agencies periodically. You are entitled to obtain a free annual credit report from each of the nationwide credit reporting companies—Equifax, Experian, and TransUnion. To do so, please go to [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 1-877-322-8228. If you notice any suspicious activity, you should promptly report such activity to the proper law enforcement agencies.

We also recommend that you consider placing a fraud alert on your credit files. Adding a fraud alert to your credit report file makes it more difficult for someone to get credit in your name by requiring creditors to follow certain procedures. However, this may also delay your ability to obtain credit. No one is allowed to place a fraud alert on your credit report except you, so if you elect to do so, please follow the instructions below to place

the alert. To place a fraud alert on your file, contact one of the three nationwide credit reporting agencies; the first agency that processes your fraud alert will notify the others to do so as well. You may also add a security freeze to your credit report file to prohibit a credit reporting agency from releasing information from your credit report without your prior written authorization. In some cases, agencies may charge a fee to place or remove such a freeze.

**Equifax**

P.O. Box 740241  
Atlanta, GA 30374  
www.equifax.com  
1-800-525-6285

**Experian**

P.O. Box 9532  
Allen, TX 75013  
www.experian.com  
1-888-397-3742

**TransUnion**

Fraud Victim Assistance Division  
P.O. Box 6790  
Fullerton, CA 92834  
www.transunion.com  
1-800-680-7289

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 and *promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities*, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC").

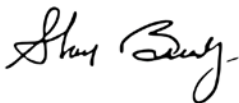
You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

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

**For More Information**

If you have any questions, please contact us at 323-785-2430.

Sincerely,



Sharon Bialy  
Bialy/Thomas & Associates