



440 East Middlefield Road
Mountain View, CA 94043

January 27, 2017



##C5816-L01-0123456 0001 00000001 *****9-OELZZ 123

SAMPLE A SAMPLE
123 ANY ST
ANYTOWN, US 12345-6789



Re: Notice of Data Breach

Dear Sample A Sample:

I am writing to make you aware of a recent email spoofing attack that may affect the security of your personal information. If you are a current employee of Company XYZ, you received a preliminary notice regarding this incident. We take this incident very seriously and are providing you with information and access to resources so that you can protect your personal information, should you feel it is appropriate to do so.

What Happened? On January 20, 2017, we learned that one of our employees had received a phishing email, which the employee mistakenly believed to be a legitimate email from an eHealth executive. As a result of the phishing email, copies of 2016 employee W-2 forms were provided before we discovered that the request was made from a fraudulent account. Since we discovered this incident, we have been working to investigate and mitigate its potential impact.

What Information Was Involved? A file containing a copy of your IRS Tax Form W-2, was sent in response to the fraudulent email. An IRS Tax Form W-2 includes the following types of information: (1) the employee’s name; (2) the employee’s address; (3) the employee’s Social Security number; and (4) the employee’s wage information. No other types of information, such as bank account information or credit card information, were exposed.

What We Are Doing. The confidentiality, privacy, and security of our employee information is one of our highest priorities. Company XYZ has stringent security measures in place to protect the security of information in our possession. Although our investigation is ongoing, there is no evidence that the individuals who sent the fraudulent emails accessed our computer network or that our IT systems were otherwise compromised by this attack. As part of our ongoing commitment to the security of personal information in our care, we are working to provide additional mandatory training to our employees on safeguarding the privacy and security of information on our systems. We have contacted the IRS and will be contacting certain state Attorneys General as well.

0123456



C5816-L01

We have arranged for you to have access to Experian's ProtectMyID® Elite credit and identity monitoring for 24 months at no cost to you. ***We strongly encourage you to act to take advantage of these free identity protection services as soon as possible.*** It is incumbent upon you to enroll in these services, as we are not able to act on your behalf to enroll you in the credit monitoring service.

To start monitoring your personal information please follow the steps below:

1. Ensure that you **enroll by: February 10, 2019** (Your code will not work after this date.)
2. **Visit** the ProtectMyID website to enroll: www.protectmyid.com/enroll
3. Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with fraud resolution that arose as a result of this incident or would like an alternative to enrolling in ProtectMyID online, please contact Experian's customer care team at 877-441-6943 by **February 10, 2019**. Be prepared to provide engagement number **PC106110** as proof of eligibility for the fraud resolution services.

Additional details regarding your 24-MONTH ProtectMyID Membership:

- **Experian credit report at signup:** See what information is associated with your credit file.
- **Active Surveillance Alerts:** Monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Internet Scan:** Alerts you if your information is found on sites containing compromised data.
- **Address Change Alerts:** Alerts you of changes to your mailing address
- **Fraud Resolution:** Identity Theft Resolution agents are immediately available to help you address credit and non-credit related fraud.
- **ExtendCARE:** You receive the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **\$1 Million Identity Theft Insurance*:** Provides coverage for certain costs and unauthorized electronic fund transfers.
- **Lost Wallet Protection:** Get help replacing credit, debit, and medical insurance cards.

What You Can Do. You can review the enclosed "Steps You Can Take to Prevent Identity Theft and Fraud." You can also enroll to receive the free credit monitoring and identity restoration services described above. In addition, if you have not already done so, we encourage you to file your 2016 tax return as soon as possible, and when you file, we also encourage you to file IRS Form 14039 (an identity theft affidavit) with your tax return.

For More Information: Company XYZ takes the privacy and security of the personal information in our care seriously. We sincerely regret any inconvenience or concern this incident has caused you. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 877-441-6943 (toll free), Monday through Friday 6 a.m. to 6 p.m. Pacific, and Saturday and Sunday 8 a.m. to 5 p.m. Pacific.

Sincerely,



Dave Francis,
Chief Financial Officer &
Chief Operations Officer

STEPS YOU CAN TAKE TO PREVENT IDENTITY THEFT AND FRAUD

While we continue to investigate, you may take direct action to further protect against possible identity theft or financial loss.

We encourage you to file your tax return as soon as possible, if you have not already done so. If you have not already filed, we encourage you to file IRS Form 14039 with your 2016 tax return. You can also contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to prevent a fraudulent tax return from being filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports and explanation of benefits forms for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a “fraud alert” on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
800-680-7289
www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer’s credit report without the consumer’s written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, list, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
<https://www.freeze.equifax.com>

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/

0123456



C5816-L01

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. **For Maryland residents**, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. **For North Carolina residents**, the Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov. **For Rhode Island residents**, the Attorney General can be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov. A total of one (1) Rhode Island resident may be impacted by this incident. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement. This notice was not delayed by a law enforcement investigation.