MULLEN COUGHLIN LLC

Christopher J. DiIenno
Office: 267-930-4775
Fax: 267-930-4771
Email: cdiienno@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

January 27, 2017

VIA U.S. 1st CLASS MAIL

Attorney General Joseph Foster
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Attorney General Foster:

We represent eHealthInsurance Services, Inc. ("eHealth"), 440 E. Middlefield Road, Mountain View, CA 94043 and are writing to notify your office of an incident that may affect the security of personal information relating to nineteen (19) New Hampshire residents. The investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, eHealth does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Event

eHealth was the targeted victim of social engineering using an email spoofing or spear-phishing attack on January 20, 2017, by an individual pretending to be an eHealth executive. A request was made from what appeared to be a legitimate eHealth email for all 2016 employee W-2 information. Unfortunately, copies of all 2016 employee W-2 forms for both eHealthInsurance Services, Inc. and its subsidiary, PlanPrescriber, Inc., were provided in response to the email before the company discovered that the sender of the email was not the eHealth executive. eHealth discovered the fraudulent nature of the request on January 20, 2017, and has been working tirelessly to investigate and to mitigate the impact of the attack.

Notice to New Hampshire Residents

On January 20, 2017, eHealth provided preliminary notice to current employees via email. A copy of this notice is attached here as ***Exhibit A***. On January 27, 2017, eHealth will begin providing written notice of this incident to all affected current and former eHealthInsurance Services, Inc. and PlanPrescriber, Inc., employees, which includes nineteen (19) New Hampshire residents. Written notice will be provided in substantially the same form as the letter attached here as ***Exhibit B***.

Other Steps Taken and to Be Taken

Upon discovering the fraudulent nature of the email, eHealth moved quickly to identify those that may be affected, to put in place resources to assist them, and to provide them with notice of this incident.

eHealth is providing all potentially affected individuals access to 2 free years of credit and identity monitoring services, including identity restoration services, through Experian, and has established a dedicated hotline for potentially affected individuals to contact with questions or concerns regarding this incident. Additionally, eHealth is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. eHealth is also providing written notice of this incident to other state regulators as necessary. eHealth has provided notice of this incident to the IRS and the FBI.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4775.

Very Truly Yours,

Christopher J. DiIenno of
MULLEN COUGHLIN LLC

CJD:ncl
Enclosures

Exhibit A

This is the content of an email that was sent to all active eHealth employees at 6:24 PM on Friday, January 20 2017 under the subject Notice of Privacy Incident. It was sent by Rena Lane, VP HR with cc to Emily Lee, Legal Counsel, and Claudia Girrbach, CISO.

Dear Employees,

eHealth is committed to protecting the security and confidentiality of the personal information we maintain related to our employees and former employees. Regrettably, we are writing to inform you of an incident involving some of that information.

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, our employees' 2016 W-2 tax forms, including your name, address, Social Security number and 2016 earnings information, may have been accessed by unauthorized individuals.

We are sending this email to alert you to this incident as quickly as possible and to let you know the steps we will be taking to help protect you. We are actively working to engage a credit monitoring and identity theft protection service. We will email again as soon as we have the details on which service we will use and how you can enroll. In addition to notifying law enforcement of the incident, we will notify the IRS so that they can monitor affected accounts. We will also notify the state tax authorities.

This email will be followed by a notification letter sent to your home address in the near future, via U.S. mail, which will reiterate instructions for Company paid enrollment in a credit monitoring and identity theft protection service. More details about this service and other steps you can take to protect yourself will be provided in the letter.

W-2 statements will be posted on ADP starting on Monday, January 23. If you would like to access this information, attached to this e-mail are Frequently Asked Questions that include instructions on how to access ADP Workforce Now.

The investigation of this incident is ongoing. Accordingly, in order to not jeopardize or interfere with our investigation, including any law enforcement investigation, this email is to remain confidential and should not be shared. We thank you for your cooperation in this regard.

We deeply regret any inconvenience this incident may cause. If you have any questions in the meantime, please contact Rena Lane, VP of Human Resources at rena.lane@ehealth.com, Emily Lee, Privacy Officer at emily.lee@ehealth.com, or Claudia Girrbach, Chief Information Security Officer at claudia.girrbach@ehealth.com.

Exhibit B

eHealth®
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

C5816-L01

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	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	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	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-685-1111	1-888-397-3742	1-888-909-8872
https://www.freeze.equifax.com	www.experian.com/freeze/	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.

C5816-L01