LEWIS BRISBOIS BISGAARD & SMITH LLP
ATTORNEYS AT LAW

550 E. Swedesford Road, Suite 270
Wayne, Pennsylvania 19087
Telephone: 215.977.4100
Fax: 215.977.4101
www.lewisbrisbois.com

CHRIS DIIENNO
DIRECT DIAL: 215.977.4059
CHRIS.DIIENNO@LEWISBRISBOIS.COM

April 7, 2016

VIA U.S. 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 Security Incident**

Dear Attorney General Foster:

We represent Asure Software ("Asure"), 110 Wild Basin Road, Suite 100, Austin, TX 78746, and are writing to notify you of a data security incident that may affect the security of personal information of one (1) New Hampshire resident. This notice will be supplemented if any new significant facts arise subsequent to its submission. By providing this notice, Asure does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Security Event

On March 7, 2016 Asure was the victim of an email phishing attack and an unidentified third party obtained access to Asure employees' W-2 information for calendar year 2015. The W-2's contained (1) employee name; (2) employee address; (3) employee Social Security number; and (4) employee wage information. The phishing attack was discovered on March 17, 2016.

Notice to New Hampshire Residents

Written notice was provided to the one (1) New Hampshire resident whose information was subject to unauthorized access on March 29, 2016, in substantially the same form as the letter attached hereto as ***Exhibit A***. A preliminary email notice was also provided on March 28, 2016 in substantially the same format as ***Exhibit B***.

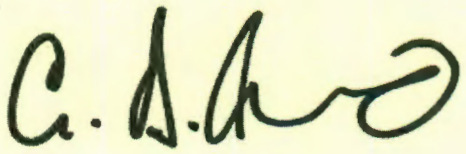
Other Steps Taken and To Be Taken

In addition to providing notice of this incident to all affected individuals as described above, Asure is providing affected individuals with twelve (12) months of credit monitoring services, along with helpful information on how to protect against identity theft and fraud. Asure is also providing written notice of this incident to other state regulators where required. To help prevent another incident of this kind, Asure is reviewing its processes, reminding staff regarding how to guard against phishing and other suspicious email, and enhancing its policies and procedures.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 215-977-4059.

Very truly yours,



Chris DiIenno of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl.

EXHIBIT A

ASURESOFTWARE

RE: Notice of Data Breach

We are writing to inform you about an incident involving the security of your personal information contained on Internal Revenue Service (IRS) Tax Form W-2. We are providing this notice to ensure that you are aware of the incident so that you may take steps to protect your personal information should you feel it is appropriate to do so.

What Happened? On Monday, March 7, 2016, Asure Software was the target of a phishing attack in which hackers posing as an Asure executive successfully requested employee W-2 information via email. Unfortunately, the W-2s were provided before it was discovered that the request was made by what appeared to be the Asure executive's email address. We discovered the fraudulent nature of this request on Thursday, March 17 and have been working tirelessly to investigate and to mitigate the impact of the attack.

What Information Was Involved? Your IRS Tax Form W-2 was sent in response to the fraudulent email request. An IRS Tax Form W-2 includes the following categories of information:
(1) employee name; (2) employee address; (3) employee Social Security number; and (4) employee wage information.

What We Are Doing. We take this incident, and the security of your personal information, very seriously. Asure has stringent security measures in place to protect the security of information in our possession. As part of our ongoing commitment to the security of personal information in our care, we are working to implement additional safeguards and provide additional mandatory training to our employees on safeguarding the privacy and security of information on our systems.

In addition to notifying all employees impacted by this incident, we have notified the IRS and law enforcement. Additionally, we are offering all affected employees one (1) year of free credit monitoring and identity restoration services with Experian. The enclosed Privacy Safeguards Information contains instructions on how to enroll and receive these free services, as well as more information on how to better protect against identity theft and fraud.

ASURESOFTWARE

What You Can Do? You can review the enclosed Privacy Safeguards Information. You can also enroll to receive the twelve (12) months of free credit monitoring and identity restoration services.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call us at 888-323-8835 x 2678, or email Cheryl Trbula, Director of Human Resources, at crbula@asuresoftware.com.

Asure takes the privacy of its employees' personal information seriously. We sincerely regret the inconvenience and concern this incident has caused you.

Sincerely,

Cheryl Trbula, SHRM-CP
Director of Human Resources | Asure Software
110 Wild Basin Rd | Suite 100 | Austin, TX 78746
E: ctrbula@asuresoftware.com
O: 888-323-8835 x 2678
M: 512-731-6332
F: 512-437-2365
asuresoftware.com

ASURESOFTWARE

PRIVACY SAFEGUARDS INFORMATION

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

We encourage you to file your tax returns 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 2015 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.

Please note that if you have received a refund anticipation loan or treasury check in relation to your 2015 taxes, the IRS recommends you not cash the check until your tax return has processed.

We also encourage you to enroll in the credit and identity monitoring services by following the enrollment instructions below:

Activate ProtectMyID Now in Three Easy Steps

1. ENSURE That You Enroll By: **June 30, 2016** (Your code will not work after this date.)
2. VISIT the ProtectMyID Web Site to enroll: **http://www.protectmyid.com/protect**
3. PROVIDE Your Activation Code:

If you have questions or need an alternative to enrolling online, please call **866-751-1324** and provide engagement #: **PC100387**.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH 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 Credit Monitoring: Alerts of key changes & suspicious activity found on your Experian, Equifax®, and TransUnion® 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, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance:** 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 Elite is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID Elite, 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 866-751-1324.

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 Security Freeze
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
1-800-685-1111	1-888-397-3742	888-909-8872
www.equifax.com/help/credit-freeze/en_cp	www.experian.com/freeze/center.html	www.transunion.com/freeze

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, www.ncdoj.gov. For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us. 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. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. 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.

EXHIBIT B

Dear Colleagues:

I am writing to notify you of an event affecting the security of your personal information. We are notifying you so you can take action along with our efforts to minimize or mitigate any potential harm. We strongly recommend you take the preventative measures listed below to better protect against misuse of your personal information.

What happened

On Monday, March 7, 2016, Asure Software was the target of a phishing attack in which hackers posing as an Asure executive successfully requested employee W-2 information via email. Unfortunately, the W-2s were provided before it was discovered that the request was made by what at first glance appeared to be the Asure executive's email address. We discovered the fraudulent nature of these requests on Thursday, March 17 and have been working tirelessly to investigate and to mitigate the impact of the attacks. As part of our response, we have notified law enforcement and the IRS.

What You Can Do:

We are currently arranging for you to have access to complimentary credit monitoring and identity restoration services, and will provide you with instructions to receive these services shortly. In the meantime, we recommend you take the following preventative measures:

- **File** your taxes as soon as possible, if you have not already. You should also file an IRS Identify Theft Affidavit (IRS Form 14039). Select Box 2A on the form. By submitting this form you are formally notifying the IRS that you are a potential victim of identify fraud and would like to mark your account to identify any questionable behavior.

- **Contact the IRS** at 1-800-908-4490" target="_blank">1-800-908-4490. Visit https://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 https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

- **Monitor your financial accounts carefully**, and if you see any unauthorized activity, promptly contact your bank, credit union, or credit card company. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain.

- **Monitor your credit reports** for suspicious or unauthorized activity. Under U.S. law, individuals are entitled to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228" target="_blank">1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report:

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
800-525-6285" target="_blank">800-525-6285	888-397-3742" target="_blank">888-397-3742	800-680-7289" target="_blank">800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

- **Contact law enforcement** to report suspicious activity or incidents of identity theft and fraud.

- **If you suspect unauthorized activity, place a "fraud alert" or a "credit freeze" on your credit reports.** You can find out more information from the Federal Trade Commission about fraud alerts and freezing your credit files, at: articles/0497-credit-freeze-faqs" target="_blank">https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs). To place a fraud alert or freeze on your credit files, contact the three credit reporting agencies listed above. Placing a fraud alert entitles you to free copies of your credit reports. A fraud alert is a signal placed in your credit report to warn potential creditors that they must use what the law calls "reasonable policies and

procedures" to verify your identity before they issue credit in your name. To find our more on how to place a security freeze, you can use the following contact information:

- Equifax: P.O. Box 105788, Atlanta, GA 30348, 800-685-1111" target="_blank">800-685-1111, http://www.equifax.com/help/credit-freeze/en_cp
- TransUnion: P.O. Box 2000, Chester, PA 19022, 888-909-8872" target="_blank">888-909-8872, www.freeze.transunion.com
- Experian: P.O. Box 9554, Allen, TX 75013, 888-397-3742, https://www.experian.com/freeze/center.html

We are very sorry for any inconvenience or concern this incident causes you. The security of your information is a priority to us, and we are taking steps to prevent an incident like this from happening again. You will be receiving a follow up letter from us in the mail with instructions for enrollment in credit monitoring services as well as reiterating steps you can take to protect yourself. If you have any questions please contact me via email and I will do our best to reply within 48 hours; however, please understand that we are working with the appropriate authorities and with legal counsel to provide you with the resources and information you will need to address this, and that we will be providing this additional information to you shortly.