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

JAMES E. PRENDERGAST
DIRECT DIAL: 215.977.4058
JIM.PRENDERGAST@LEWISBRISBOIS.COM

April 18, 2016

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 Event

To Attorney General Foster:

We represent Client Network Services, Inc., 2277 Research Blvd., Rockville, MD 20850 and are writing to notify you of a data security incident that may have compromised the security of personal information of one (1) New Hampshire resident. By providing this notice, Client Network Services, Inc. does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Security Event

On Thursday, March 23, 2016, Client Network Services, Inc. discovered that it was the victim of an email spoofing attack by an individual purporting to be their CEO. Through this attack, a request was made from what appeared to be a legitimate Client Network Services, Inc. email address for 2015 employee W2 information. Unfortunately this information was provided before Client Network Services, Inc. discovered that the request was fraudulent. Client Network Services, Inc. immediately reported this incident to law enforcement and are cooperating with their ongoing investigation.

Notice to the Affected New Hampshire Resident

While Client Network Services, Inc.'s investigation continues, Client Network Services, Inc. is taking appropriate steps to notify individuals potentially affected by this incident. Client Network Services, Inc. has identified one (1) New Hampshire resident whose name, Social Security number; and employee's wage and tax withholding information were affected by this incident. On April 8, 2016, Client Network Services, Inc. mailed a notice letter to the affected New Hampshire resident. Attached as ***Exhibit A*** is an exemplar of the notice letter that was mailed to the affected individual.

Other Steps Taken and To be Taken

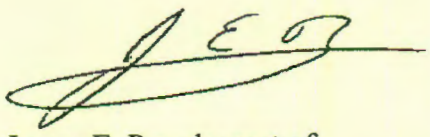
Client Network Services, Inc. takes this incident, and the security of the personal information in our care, very seriously. As part of our ongoing commitment to the security of personal information, we are working to implement additional safeguards and provide additional mandatory training to our employees on safeguarding the privacy and security of information on our systems.

To support potentially affected individuals, on April 8, 2016 a toll-free hot-line was established to answer questions about this incident and to provide information relating to protection against identity theft and fraud. Client Network Services, Inc. will provide affected individuals access to a two (2) year membership to credit monitoring and identity protection services through AllClear, at no cost to the affected individual.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security compromise and response, please contact me at 215-977-4058.

Very truly yours,



James E. Prendergast of
LEWIS BRISBOIS BISGAARD & SMITH LLP

JEP:ncl
Enclosures

EXHIBIT A

CNSI
Processing Center • P.O. BOX 141578 • Austin, TX 78714

00001
ACD1234
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

April 8, 2016

Re: Notice of Data Security Event

Dear John Sample,

I am writing to follow up my March 23rd email correspondence to you regarding the February 25, 2016 email spoofing attack that occurred at CNSI. As you know, we take this incident very seriously and are writing to provide you with more information and access to resources so that you can protect your personal information.

What Happened? We recently discovered that our company was the victim of an email spoofing attack by an individual purporting to be our CEO. Through this attack, a request was made from what appeared to be a legitimate CNSI email address for 2015 employee W2 information. Unfortunately this information was provided before we discovered that the request was fraudulent. We discovered the fraudulent nature of this request on Wednesday, March 23, and have been working to investigate and to mitigate the impact of the attacks.

What Information Was Involved? An abstract of CNSI's 2015 W2 information was sent in response to the fraudulent email proving the following data elements: (1) the employee's name; (2) the employee's Social Security number; and, (3) the employee's wage and tax withholding information.

What We Are Doing? We take this incident, and the security of your personal information, very seriously. As part of our ongoing commitment to the security of personal information in our care, we are working to strengthen existing safeguards and provide additional mandatory training to our employees on recognizing fraudulent emails and safeguarding the privacy and security of information on our systems. We have contacted the IRS, and will be contacting the relevant state Attorneys General.

Additionally, we are offering all affected individuals access to 24 months of free credit monitoring and identity restoration services with AllClear ID. The enclosed Steps You Can Take To Prevent Identity Theft And Fraud contains instructions on how to enroll to receive these free services, as well as more information on how to better protect against identity theft and fraud.

01-02-1-00

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 24 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. We have established a confidential, toll free hotline to assist with questions regarding this incident, this letter or AllClear ID identity monitoring and protection services. This hotline can be reached at 1-855-731-6018, Monday-Saturday, 8:00 a.m. – 8:00 p.m. Central Standard Time.

Client Network Services, Inc. takes the privacy of the personal information in our care seriously. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

Arnold Morse
Senior Vice President, General Counsel
Client Network Services, Inc.

STEPS YOU CAN TAKE TO PREVENT IDENTITY THEFT AND FRAUD

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.

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 SECURE: The team at AllClear ID is ready and standing by if you need identity repair assistance. This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-731-6018 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear PRO: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. For a child under 18 years old, AllClear ID ChildScan identifies acts of credit, criminal, medical or employment fraud against children by searching thousands of public databases for use of your child's information. To use the PRO service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-731-6018 using the following redemption code: Redemption Code.

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your bank and credit card account statements, and to monitor your credit reports and explanation 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
(NY residents please call 1-800-349-9960)	www.experian.com/freeze/center.html	www.transunion.com/freeze
www.equifax.com/help/credit-freeze/en_cp		

The Federal Trade Commission (FTC) encourages those who discover that their information has been misused to file a complaint with them. To file a complaint with the FTC, or to obtain additional information on identity theft and the steps that can be taken to avoid identity theft, the FTC can be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580, or at www.ftc.gov/idtheft, or (877) ID-THEFT (877-438-4338); TTY: (866) 653-4261. This notice has not been delayed because of law enforcement; however, instances of known or suspected identity theft should be reported to law enforcement, the Attorney General in the individual's state of residence, and the FTC. State Attorneys General may also have advice on preventing identity theft. Employees can also learn more about placing a fraud alert or security freeze on their credit files by contacting the FTC or their state's Attorney General. **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, 1-888-743-0023, www.oag.state.md.us.