



MULLEN COUGHLIN... STATE OF NH DEPT OF JUSTICE

2017 MAR 31 AM 11:48
1275 Drummers Lane, Suite 302
Wayne, PA 19087

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

March 27, 2017

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

Re: Notice of Data Security Incident

Dear Attorney General Foster:

We represent Language Services Associates, Inc. ("LSA"), 455 Business Center Drive, Suite 100, Horsham, Pennsylvania 19044, and are writing to notify you of a recent incident that may affect the security of the personal information of 2 New Hampshire residents. The investigation into this incident is ongoing and will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, LSA does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Security Incident

On February 10, 2017, LSA became aware of unauthorized access to its Human Resources Director's email account after that email account was used by an unknown actor to send out malicious "phishing" emails to LSA employees and other individuals on that same date. In response, LSA immediately launched an investigation and brought in outside computer forensics experts to confirm the security of its systems and determine whether any information was subject to unauthorized access. It was determined that the HR Director's email account was subject to unauthorized log-ins by an unknown individual on February 4 and February 10, 2017. A thorough forensic investigation by outside experts has found no other compromise of LSA's information systems aside from the unauthorized access to the HR Director's email account.

While no forensic evidence has been found that any personal information stored within the HR Director's email account was actually viewed or accessed by the unknown individual, such activity could not be ruled out. Therefore, an intensive forensic review of the email account's contents was performed to identify all individuals for whom personally identifiable information ("PII") was contained within those email accounts. The large volume and variety of documents in need of review required a combination of automated forensic tools and manual document review by a forensics expert to check the data contents for the presence of PII. Once all potentially affected individuals were identified, LSA engaged in an additional process of confirming address information for a portion of the population, which involved a review of LSA's internal records and National Change of Address ("NCOA") database address verification provided by an outside vendor. In an effort to directly provide written notice of this incident to as many potentially affected individuals as possible, LSA took the above steps as expediently as possible after discovering this incident.

While the types of PII determined to be stored within the HR Director's email account were not identical for every potentially affected individual, the vast majority only had their name and Social Security found within the email account.

Notice to New Hampshire Residents

On March 27, 2017, LSA mailed written notice of this incident to potentially affected individuals, including 2 New Hampshire residents whose name and Social Security number were determined to be stored within the email account. Such notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken

LSA is offering potentially affected individuals complimentary access to 24 months of free credit monitoring and identity protection services with AllClear ID, as well as information on how to protect against identity theft and fraud, including information on how to contact the Federal Trade Commission, the state attorney general, and law enforcement to report any attempted or actual identity theft and fraud. In addition to providing notice of this incident to you, LSA reported this incident to local law enforcement and is providing written notice of this incident to other state regulators where required.

Since discovering this incident, LSA has implemented the following measures to enhance protections against this type of incident moving forward:

- Organization-wide email account password update;
- Upgrading their firewall;
- Blocking the malicious IP addresses associated with this incident from their systems;
- Quarantining and confirming the security of any computers affected by this incident;
- Updating protection software and antivirus/antimalware scanning on all computers across the organization;
- Increased spam filtering for its email system;
- Additional proactive monitoring of its systems.

Contact Information

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

Very Truly Yours,



Christopher DiLenno of
MULLEN COUGHLIN LLC

CJD:ab
Enclosure

Exhibit A



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



00048
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

March 27, 2017

Re: Notice of Data Breach

Dear John Sample:

Language Services Associates, Inc. (“LSA”) is writing to notify you of a recent incident that may affect the security of your personal information. Although we are unaware of any actual or attempted misuse of your information, we are providing you with information regarding the incident, steps we have taken since discovering the incident, and what you can do to protect against identity theft and fraud should you feel it is appropriate to do so.

What Happened? On February 10, 2017, LSA became aware of unauthorized access to our HR Director’s email account after that account was used by an unknown individual to send out a malicious “phishing” email to LSA employees and others on February 10, 2017. In response, LSA immediately launched an investigation and brought in outside computer forensics experts to confirm the security of our systems and determine whether any information was subject to unauthorized access. It was determined that the HR Director’s email account was subject to unauthorized log-ins by an unknown individual on February 4, 2017 and February 10, 2017. Our investigation has found no other compromise of our information systems aside from the unauthorized access to the HR Director’s email account.

What Information Was Involved? While no evidence has been found that any personal information stored within the HR Director’s email account was viewed or removed by the unknown individual, our investigation cannot rule out that this type of activity happened. Therefore, we are providing this notice to you in an abundance of caution. Our investigation determined that the types of your information that were accessible due to the unauthorized access to the email account included the following: name, and Social Security number.

What We Are Doing. At LSA we take your privacy and the security of the personal information within our care very seriously. We are taking steps to enhance data security protections to prevent similar incidents in the future. We are also notifying certain government regulators about this incident.

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.



01-02-6-00

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-501-5689 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. To use this 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 1-855-501-5689 using the following redemption code: Redemption Code.

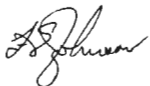
Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

What You Can Do. You can enroll in the AllClear ID credit monitoring service using the enrollment information above. You can also review the enclosed *Steps You Can Take to Protect Against Identity Theft and Fraud*, which includes guidance on steps you can take to better protect against the possibility of fraud and identify theft.

For More Information: We recognize that you may have questions that are not answered in this letter. If you have questions or concerns that are not addressed in this notice letter, you may call the dedicated call center we've established regarding this incident at 1-855-501-5689. The call center is available Monday through Saturday, 9:00 a.m. to 9:00 p.m. E.D.T. (excluding U.S. holidays).

We sincerely regret any inconvenience this incident may cause. LSA remains committed to safeguarding information in our care and will continue to take proactive steps to enhance data security.

Sincerely,



Frank Johnson
President

Steps You Can Take to Protect Against Identity Theft and Fraud

In addition to enrolling to receive the services detailed above, you may take action directly to further protect against possible identity theft or financial loss. 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
1-800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-680-7289
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, lift 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
(NY residents please call
1-800-349-9960)
<https://www.freeze.equifax.com>

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
[www.experian.com/freeze/
center.html](http://www.experian.com/freeze/center.html)

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
1-888-909-8872
www.transunion.com/credit-freeze

Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. You can further educate yourself regarding identity theft, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/idtheft, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your state's 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 at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-919-716-6400, 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 3 Rhode Island residents may be impacted by this incident.