



MULLEN
COUGHLIN_{LLC}

STATE OF NH
DEPT OF JUSTICE
2017 MAY -1 AM 11:13

James E. Prendergast
Office: 267-930-4798
Fax: 267-930-4771
Email: jprendergast@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

April 25, 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 KeraLink International (“KeraLink”), 5520 Research Park Drive, Suite 400, Baltimore, MD. We 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. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, KeraLink does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Security Event

On or around April 6, 2017, a human resources assistant received a spoofed email requesting PDF copies of the 2016 W2s for current and former employees of KeraLink. The employee responded to the spoofed email attached PDF copies of all 2016 W2s for current and former employees of KeraLink. On or around April 6, 2017, KeraLink’s Chief Executive Officer was alerted to the spoofing attack when the human resources assistant asked if he received her email of the W2 copies. KeraLink immediately launched an investigation and have been working tirelessly to investigate and to mitigate the impact of the attack.

Notice to New Hampshire Resident

On April 7, 2017, KeraLink provided preliminary notice by way of email, if an email address was available, and posting on KeraLink’s internal communication system. The notice was provided in substantially the same form as the email attached here as **Exhibit A**. On April 25, 2017,

Mullen.law

Attorney General Joseph Foster
April 25, 2017
Page 2

KeraLink mailed notice letters to individuals, including one (1) New Hampshire resident, whose personal information was compromised in the W2 phishing scam. The notice was provided in substantially the same form as the letter attached here as ***Exhibit B***.

Other Steps Taken

Once KeraLink discovered the incident, they took immediate steps to respond and to protect the information at issue. KeraLink is internally reviewing employee training curriculum with regard to phishing scams.

KeraLink is providing all potentially affected individuals access to 1 free years of credit and identity monitoring services, including identity restoration services, through ID Experts. Additionally, KeraLink 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. KeraLink is also providing written notice of this incident to other state regulators as necessary. The IRS and FBI have also been notified of this event.

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4798.

Very truly yours,



James E. Prendergast of
MULLEN COUGHLIN LLC

JEP:ncl
Enclosures

Exhibit A

STATE OF NH
DEPT OF JUSTICE
2017 MAY -1 AM 11:13

MEMORANDUM

TO: Individuals Employed by KeraLink International in 2016
DATE: April 7, 2017
RE: URGENT COMMUNICATION – Preliminary Notice of Data Incident

We recently discovered that our company was the victim of an email spoofing attack on April 6, 2017, by an individual pretending to be our Chief Executive Officer, Doug Furlong. A fraudulent email request was made that all 2016 KeraLink International employee W-2 information be forwarded to someone purporting to be KeraLink International's auditor. Unfortunately, copies of all 2016 employee W2 forms were provided before we discovered that the request was made from a fraudulent account. We discovered the fraudulent nature of the request on April 6, 2017 and have been working tirelessly to investigate and to mitigate the impact of the attack. This type of theft is usually meant to generate the information needed to file a phony tax return in the taxpayer's name in order to fraudulently obtain a tax refund.

Please note that this incident affects you only if you were employed by KeraLink International in 2016. If your employment did not begin with KeraLink International until 2017, then your information has not been impacted.

The confidentiality, privacy, and security of our employee information is one of our highest priorities. While our investigation is ongoing, we felt it important to notify you about this incident, and what we are doing to investigate and respond, as quickly as possible. Here are some actions that we are taking and that we encourage you to take:

- **Identity Protection.** As a precaution, for those individuals affected by this incident, we are arranging for credit monitoring services to protect your identify for 12 months at no cost to you. The cost of this service will be paid for by KeraLink International and instructions for activating your protection will be included in a forthcoming letter. ***We strongly encourage you to act to take advantage of these free identity protections 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.
- **Immediate Steps.** You may place a "fraud alert" or a "credit freeze" on your credit reports by contacting one of the three credit reporting agencies. You can learn more about the process and procedure by visiting the three credit bureaus listed below. If you have been a victim of identity theft, and you provide each 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. If you are charged such a fee in setting up a credit freeze that is not waived, please let us know and we will reimburse you directly. The three credit reporting agencies are Equifax (800-525-6285) - www.equifax.com; Experian (888-397-3742) - www.experian.com; and TransUnion (800-680-7289) - www.transunion.com. You can also find out more information from the Federal Trade Commission at www.identitytheft.gov regarding fraud alerts and freezing your credit files.

- Notice to Affected Individuals. We also will be mailing information to all impacted current and former KeraLink team members.
- Employee Questions. You may reach Ed Cordell, CFO, at 404-641-3439 (ecordell@keralink.org).
- Notice to Law Enforcement and the IRS. We have notified federal law enforcement of the incident, and we will be notifying any necessary state Attorneys General as well. We also are reporting this incident to the IRS so that they may take steps to monitor for attempts to file fraudulent tax returns using KeraLink International employee information. We will also take steps, as necessary, to notify appropriate state taxing authorities of the incident.
- Filing of 2016 Tax Returns. We encourage you to file your 2016 tax return as soon as possible, if you have not already done so. You can contact the IRS at <http://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.
- Employee Training. Unfortunately, even the best technology cannot prevent all cyber-attacks, particularly those intended to fool employees into providing sensitive company information. We will continue and improve upon our information security awareness and training programs for all employees.

We apologize for any inconvenience this incident causes you. Please know that we are working diligently to remedy this incident and to prevent any similar incidents from occurring in the future. If you have any questions about the contents of this notice or about the incident, please contact Ed Cordell, CFO, at 404-641-3439 (ecordell@keralink.org).

Exhibit B



Advancing Corneal Transplantation

C/O ID Experts
10300 SW Greenburg Ste. 570
Portland, OR 97223

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

April 25, 2017

Re: Notice of Data Breach

Dear <<First Name>>:

I am writing to make you aware of a recent email spoofing attack that may affect the security of your personal information. We take this 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? We recently discovered that our company was the victim of an email spoofing attack on April 6, 2017, by an individual pretending to be our Chief Executive Officer. A request was made for all 2016 KeraLink International employee W-2 information. Unfortunately, copies of all 2016 employee W-2 forms were provided before we discovered that the request was made from a fraudulent account by someone purporting to be our CEO. We discovered the fraudulent nature of the request on April 6, 2017 and have been working continuously since then to investigate and to mitigate the impact of the attack.

What Information Was Involved? A file, including 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 categories 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. Other than information contained on the IRS Tax Form W-2, no personal financial information was emailed to the external email account.

What We Are Doing. KeraLink International has stringent security measures in place to protect the security of information in our possession. The confidentiality, privacy, and security of our employee information is one of our highest priorities. At this time, we do not believe that the individual who sent the fraudulent email accessed our computer network or that our IT systems were otherwise compromised by this attack. In addition, 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. We have contacted the IRS and FBI and will be contacting the relevant state Attorneys General.

As an added precaution, we have arranged to have ID Experts® protect your identity for 12 months at no cost to you. ID Experts' MyIDCare services include: Credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, exclusive educational materials and fully managed id theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised. The cost of this service will be paid for by KeraLink International. 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.

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 1-800-939-4170 or going to www.idexpertscorp.com/protect and using the Enrollment Code provided below. MyIDCare experts are available Monday through Friday from 6 am - 5 pm Pacific Time. Please note the deadline to enroll is July 26, 2017.

Your Enrollment Code: <<Enrollment Code>>

We encourage you to take full advantage of this service offering. MyIDCare representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

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.

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 1-800-939-4170 Monday through Friday 6 am - 5 pm Pacific Time to speak to a MyIDCare expert.

KeraLink International 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.

Sincerely,

A handwritten signature in blue ink that reads "Douglas J. Furlong". The signature is written in a cursive style with a large, stylized 'D' and 'F'.

Douglas J. Furlong
Chief Executive 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. 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 19106
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
<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/

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); and TTY: 1-866-653-4261.

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 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 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. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.