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

June 16, 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 Event**

Dear Attorney General Foster:

We represent the Foundation of the Massachusetts Eye and Ear Infirmary, Inc., Massachusetts Eye and Ear Infirmary, and Massachusetts Eye and Ear Associates, Inc., 243 Charles Street, Boston, MA 02214 (collectively "Mass. Eye and Ear"), and are writing to notify your office of an incident that affects the security of personal information relating to fifty-three (53) New Hampshire residents. The investigation into this event is ongoing and this notice will be supplemented with substantive facts learned subsequent to this submission. By providing this notice, Mass. Eye and Ear does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Event

In late April 2016, Mass. Eye and Ear began investigating reports of IRS tax fraud based on comments from several employees. Upon discovering anomalies in the logs of their UltiPro HR system on May 3, 2016, which they confirmed were instances of unauthorized access on May 4, 2016, Mass. Eye and Ear launched a full forensic investigation into the nature and scope of the potential intrusion. The Mass. Eye and Ear IT team worked with third party forensic investigators and with the UltiPro provider to identify those individuals whose information was affected, as well as the data that was compromised. Through this investigation, Mass. Eye and Ear confirmed that there was a compromise of some of the personal information stored in the UltiPro HR system. Through this compromise, between March 21 and May 4, 2016, an unauthorized individual used stolen administrator credentials to gain access to the UltiPro HR system and view sensitive information. On June 1, 2016, Mass. Eye and Ear was able to confirm, working with third party forensic investigators, as well as the UltiPro provider, the names of those individuals whose information was the subject of the unauthorized access and the nature of the sensitive personal information that was viewed for each of the impacted individuals. Mass. Eye and Ear has been

working diligently to investigate and to mitigate the impact of the attack since they discovered this intrusion into the system. This incident affected certain current and former employees and certain employee spouses, beneficiaries, and dependents. It did NOT affect any patient data.

Notice to New Hampshire Residents

On April 29, 2016, Mass. Eye and Ear sent email notice to potentially affected employees, informing them that they were investigating reports of tax fraud. This notice was provided in substantially the same form as the letter attached hereto as ***Exhibit A***. On May 23, 2016, after discovering the UltiPro intrusion, but prior to identifying those individuals who were directly impacted, Mass. Eye and Ear emailed preliminary notice to all current employees for whom they were able to determine valid email addresses informing them that they were investigating the potential compromise of their personal information. This notice was provided in substantially the same form as the letter attached hereto as ***Exhibit B***. On June 16, 2016, Mass. Eye and Ear will send an additional email notice to all employees for whom they are able to determine valid email addresses; informing them that the impacted individuals have been identified and will be receiving written notice in the mail. This notice will be provided in substantially the same form as the letter attached hereto as ***Exhibit C***. On June 16, 2016, Mass. Eye and Ear will mail notice letters to all impacted individuals, which includes fifty-three (53) New Hampshire residents. The notifications provide details of the incident, information on steps individuals can take to protect against identity theft and fraud, access to two (2) years of free credit monitoring and identity theft restoration assistance, and contact information individuals may use should they have questions or concerns. The notice letter will be provided in substantially the same form as the letters attached here as ***Exhibit D.***

Other Steps Taken and To Be Taken

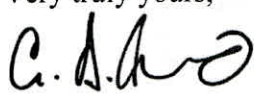
Upon discovering this incident, Mass. Eye and Ear moved quickly to identify those that may be affected, to put in place resources to assist them, and to provide them with notice of this incident. As noted above, Mass. Eye and Ear is providing impacted individuals with two (2) years of free credit monitoring and identity theft restoration assistance, information on how to better protect against identity theft and fraud, including information on how to place a fraud alert or security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies and the IRS, and encouragement to contact the Federal Trade Commission, state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Mass. Eye and Ear has notified the IRS of this incident, as well as other appropriate state regulators. Since this incident was discovered, Mass. Eye and Ear changed certain user credentials with access to UltiPro, has implemented multifactor identity verification for its UltiPro system and has eliminated web-access to UltiPro (now, only users connected to the Mass. Eye and Ear system can log in to UltiPro). Mass. Eye and Ear is also reviewing its policies and procedures relating to data privacy and is taking steps to implement additional security measures and further educate its staff on data privacy related issues. Additionally, Mass. Eye and Ear continues to work with a third-party forensic team to aid in the investigation of this incident, as well as to provide guidance on any additional steps that can be taken to safeguard information in Mass. Eye and Ear's systems.

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

CJD:sn
Enclosures

EXHIBIT A

From: Fowles, Heather
Sent: Friday, April 29, 2016 9:15 AM
To: All Staff
Subject: IRS Scam

As you may already be aware, many U.S. taxpayers this year have become victims of IRS tax scams, some of which include identity theft. During the last few weeks, it has come to our attention that a number of Mass. Eye and Ear employees have been victimized by this criminal activity. We are committed to protecting our patient and employee information and have been investigating this issue vigorously. Thus far, we have found no direct evidence of a breach of MEE systems, but we continue to investigate and will keep you appraised.

In the meantime, it is very important that we know if you have been affected by this. If you believe you are a victim of fraudulent activity around the filing of your federal or state tax return, please report it to my office as soon as possible.

We highly recommend that you and your families always be aware of fraudulent activity. For the latest alerts from the IRS, simply go to their website: https://www.irs.gov/uac/Tax-Scams-Consumer-Alerts.

Heather Fowles, CISA, CISSP
Director of Information Security
Massachusetts Eye & Ear Infirmary
Office: 465 Medford St, 3rd fl, Boston MA 02129
Mailing: 243 Charles Street, Boston, MA 02114-3096
Tel: [redacted]

EXHIBIT B

To: The Mass. Eye and Ear Community
From: John Fernandez, President & CEO and Executive Leadership Team
Date: May 23, 2016
Re: Employee Alert: update on IRS Scam investigation

On April 29, we let you know that we were investigating reports of IRS tax fraud based on comments from several employees. Unfortunately, we have now confirmed that there has been a compromise of personal information stored in our HR system.

We have engaged an external forensic investigator to aid in our investigation and incident response. So far, we know that an unauthorized user gained access to portions of our HR system, UltiPro, in which sensitive information is maintained. Because employee, dependent and spousal information is stored in UltiPro, it is possible that this information may have been compromised as well. Mass. Eye and Ear, with the help of forensic experts, is actively and aggressively working to determine exactly what happened and to whom. As soon as we have complete information we will provide written notice and an action plan to all affected individuals.

We strongly encourage our employees—all of you—to consider taking the preventive measures listed below to protect yourselves against the possible misuse of personal information or identity theft.

- Mass. Eye and Ear has established a call center to help answer questions regarding this incident. For more information, please contact our dedicated assistance line at (877) 202-4625, Monday through Friday, 9 a.m. to 7 p.m. EST.

- Blue Cross Blue Shield members are entitled to receive Experian's® ProtectMyID® credit monitoring product. To learn more about these services, go to www.bluecrossma.com or call 1-866-926-9803. Most financial institutions also offer similar services, i.e., banks, credit card and investment companies. We encourage you take advantage of these services. In upcoming days, Mass. Eye and Ear will notify all affected individuals by mail and, in that notice, will make credit and identity protection services available to all such individuals, regardless of whether they are Blue Cross Blue Shield members.

- 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:

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

- If you haven't already done so, we encourage you to file your tax return as soon as possible. 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.

We know this is troubling news and ask for your patience as we work as quickly as possible to carefully complete this investigation. While we have security measures in place to protect the information in our systems, we are continuously working with vendors to supplement these existing safeguards. For example, UltiPro now supports multifactor identity verification measures. When you log into UltiPro from an on-campus computer, you are required to go through the new authentication process. You will notice we have turned off web access to UltiPro. You can still connect to UltiPro from home if you remote into the Mass. Eye and Ear network and access UltiPro from your desktop. We recognize that these new controls may be inconvenient, but they have been put in place to provide enhanced protection for your information in UltiPro.

You have heard us emphasize the importance of cyber security measures throughout our entire organization. Unfortunately, the world in which we live and work is increasingly susceptible to this kind of attack. We are very sorry for the concern and inconvenience that this incident has caused. The confidentiality, privacy, and security of our employee information are our highest priorities. We promise to communicate further with affected individuals in upcoming days.

EXHIBIT C

To: The Mass. Eye and Ear Community
From: John Fernandez, President & CEO and Executive Leadership Team
Date: June 16, 2016
Re: Employee Alert: Update on IRS Scam Investigation

Thank you to our entire community for your patience as we have conducted an exhaustive investigation into unauthorized access of the Mass. Eye and Ear HR system, UltiPro.

Working with an external forensic investigation team, we have now successfully determined exactly which employee information was accessed in UltiPro by an unauthorized user. Via the U.S. Postal Service, we will send written notices to every individual who had exposure. If you receive mail from Mass. Eye and Ear over the next few days, please be sure to open it and read it carefully. The letter will contain important information about the next steps you should take.

As a reminder, even if you are not one of those employees whose information has been compromised, we strongly encourage you to take the preventive measures listed below to protect yourselves against the possible misuse of personal information or identity theft.

- Blue Cross Blue Shield members are entitled to receive Experian's® ProtectMyID® credit monitoring product. To learn more about these services, use the attached brochure or call 1-866-926-9803. Most financial institutions also offer similar services, i.e., banks, credit card, and investment companies. We encourage you to take advantage of these services. In upcoming days, Mass. Eye and Ear will notify all affected individuals by mail and, in that notice, will make credit and identity protection services available to all such individuals, regardless of whether they are Blue Cross Blue Shield members.

- 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:

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

- If you haven't already done so, file your tax return as soon as possible. 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.

Please note, web access to UltiPro will remain shut off for the foreseeable future. You can still connect to UltiPro from home if you remote into the Mass. Eye and Ear network. We recognize that these new controls may be inconvenient, but they have been put in place to provide enhanced protection of your information in UltiPro.

Mass. Eye and Ear has established a call center to help answer questions regarding this incident. For more information, please contact our dedicated assistance line at (855) 285-8908, Monday through Saturday, 9 a.m. to 9 p.m. EST.

I want to repeat to you that we are very sorry for the concern and inconvenience that this cyber-attack has caused. The confidentiality, privacy, and security of our employee information is our highest priority. We are committed to providing you with the help and resources you need to better protect yourself. If you have any questions or concerns, please reach out to your manager.

EXHIBIT D

Massachusetts Eye and Ear
Processing Center • P.O. BOX 141578 • Austin, TX 78714

02722
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

June 16, 2016

RE: Notice of Data Security Breach

Dear John Sample,

I write as a follow-up to my May 23, 2016 email about an incident that may affect the security of some of your personal information stored in Mass. Eye and Ear's Human Resources System, UltiPro. Mass. Eye and Ear takes this incident very seriously and we are following up to provide you with additional information about the incident and access to resources so that you can better protect against the possibility of identity theft and fraud, should you feel it is appropriate to do so.

What Happened? In late April 2016, we began investigating reports of IRS tax fraud based on comments from several employees. Upon discovering anomalies in the logs of our UltiPro HR system on May 3, 2016, which we confirmed were instances of unauthorized access on May 4, 2016, we launched a full forensic investigation into the nature and scope of the intrusion. Our IT team worked with third party forensic investigators to identify those individuals whose information was affected, as well as the data that was comprised. On May 23, 2016, while we were working to identify those affected, we sent preliminary notice to all employees with information on how to protect against identity theft and fraud. Unfortunately, we have now confirmed that there has been a compromise of your personal information stored in our HR system. Through this compromise, between March 21 and May 4, 2016, an unauthorized individual used stolen administrator credentials to gain access to our UltiPro system and view sensitive information. We have been working diligently to investigate and to mitigate the impact of the attack since we discovered this intrusion into our system.

What Information Was Involved? We have confirmed the information involved in this incident includes your name and Client DEF 3.

What We Are Doing. We take this incident, and the security of your personal information, very seriously. Mass. Eye and Ear has 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 protections and provide additional training on safeguarding the privacy and security of information in our systems. We are providing notice of this incident to you, and to certain state regulators, and will be reporting this incident to the IRS. Additionally, we are working with third-party forensic investigators to confirm the security of our network.

As an additional precaution, we are providing all affected individuals access to twenty-four (24) months of free credit monitoring and identity theft protection services through AllClear ID. Instructions on how to enroll are included in the enclosed *Steps You Can Take To Protect Against Identity Theft And Fraud.* We encourage you to take advantage of these services by following the instructions to enroll.

What You Can Do. You can review the enclosed *Steps You Can Take To Protect Against Identity Theft And Fraud.* You can also enroll to receive the free credit monitoring and identity restoration services through AllClear ID.

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 contact our dedicated assistance line at [redacted], Monday through Saturday, 9 a.m. to 9 p.m. ET.

The confidentiality, privacy, and security of information in our system are our highest priorities. On behalf of the executive leadership team, I want to express our sincere regret for the inconvenience and concern this incident may have caused you.

Sincerely,

John Fernandez
President & CEO

STEPS YOU CAN TAKE TO PROTECT AGAINST 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 will be providing all affected individuals access to twenty-four (24) months of free credit monitoring service through AllClear ID. The following identity protection services start on the date of this notice and you can use them at any time during the next twenty-four (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 1-855-285-8908, Monday through Saturday, 9 a.m. to 9 p.m. ET, 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. 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 1-855-285-8908, Monday through Saturday, 9 a.m. to 9 p.m. ET, using the following redemption code: Redemption Code.

Please note: While SECURE is automatically available as of the date of this notice, you must call or go online to activate the additional PRO serve at no cost to you. Also, 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 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:

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

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 above.

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

If you receive a notice from the IRS that leads you to believe that someone may have used your information, please notify the IRS's Identity Protection Specialized Unit (IPSU) immediately at 800-908-4490 or www.irs.gov/Individuals/Identity-Protection. You will also find information at https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft. IPSU employees are available to answer questions about identity theft and resolve any tax account issues that resulted from identity theft.

If you have not yet filed your 2015 tax return, do so as soon as possible and file an IRS Identify Theft Affidavit, IRS Form 14039, with your return. 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. If you have already filed your 2015 tax return and it has been accepted by the IRS, you may file the IRS Identify Theft Affidavit, IRS Form 14039, with your 2016 return next year.

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.ftc.gov/idtheft/, 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. **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, (919) 716-6400, www.ncdoj.gov. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed because of law enforcement.

Massachusetts Eye and Ear
Processing Center • P.O. BOX 141578 • Austin, TX 78714

02765
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

June 16, 2016

RE: Notice of Data Security Breach

Dear John Sample,

I write to inform you about an incident that may affect the security of some of your personal information stored in Mass. Eye and Ear's Human Resources System, UltiPro. Mass. Eye and Ear takes this incident very seriously and we are writing to provide you with information about the incident and access to resources so that you can better protect against the possibility of identity theft and fraud, should you feel it is appropriate to do so.

What Happened? In late April 2016, we began investigating reports of IRS tax fraud based on comments from several employees. Upon discovering anomalies in the logs of our UltiPro HR system on May 3, 2016, which we confirmed were instances of unauthorized access on May 4, 2016, we launched a full forensic investigation into the nature and scope of the intrusion. Our IT team worked with third party forensic investigators to identify those individuals whose information was affected, as well as the data that was compromised. Unfortunately, we have now confirmed that there has been a compromise of your personal information stored in our HR system. Through this compromise, between March 21 and May 4, 2016, an unauthorized individual used stolen administrator credentials to gain access to our UltiPro system and view sensitive information. We have been working diligently to investigate and to mitigate the impact of the attack since we discovered this intrusion into our system.

What Information Was Involved? We have confirmed the information involved in this incident includes your name and Client DEF 3.

What We Are Doing. We take this incident, and the security of your personal information, very seriously. Mass. Eye and Ear has 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 protections and provide additional training on safeguarding the privacy and security of information in our systems. We are providing notice of this incident to you, and to certain state regulators, and will be reporting this incident to the IRS. Additionally, we are working with third-party forensic investigators to confirm the security of our network.

01-02-6-00

As an additional precaution, we are providing all affected individuals access to twenty-four (24) months of free credit monitoring and identity theft protection services through AllClear ID. Instructions on how to enroll are included in the enclosed *Steps You Can Take To Protect Against Identity Theft And Fraud.* We encourage you to take advantage of these services by following the instructions to enroll.

What You Can Do. You can review the enclosed *Steps You Can Take To Protect Against Identity Theft And Fraud.* You can also enroll to receive the free credit monitoring and identity restoration services through AllClear ID.

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 contact our dedicated assistance line at [redacted] Monday through Saturday, 9 a.m. to 9 p.m. ET.

The confidentiality, privacy, and security of information in our system are our highest priorities. On behalf of the executive leadership team, I want to express our sincere regret for the inconvenience and concern this incident may have caused you.

Sincerely,

John Fernandez
President & CEO

STEPS YOU CAN TAKE TO PROTECT AGAINST 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 will be providing all affected individuals access to twenty-four (24) months of free credit monitoring service through AllClear ID. The following identity protection services start on the date of this notice and you can use them at any time during the next twenty-four (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 1-855-285-8908, Monday through Saturday, 9 a.m. to 9 p.m. ET, 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. 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 1-855-285-8908, Monday through Saturday, 9 a.m. to 9 p.m. ET, using the following redemption code: Redemption Code.

Please note: While SECURE is automatically available as of the date of this notice, you must call or go online to activate the additional PRO serve at no cost to you. Also, 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 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:

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

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 above.

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

If you receive a notice from the IRS that leads you to believe that someone may have used your information, please notify the IRS's Identity Protection Specialized Unit (IPSU) immediately at 800-908-4490 or www.irs.gov/Individuals/Identity-Protection. You will also find information at https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft. IPSU employees are available to answer questions about identity theft and resolve any tax account issues that resulted from identity theft.

If you have not yet filed your 2015 tax return, do so as soon as possible and file an IRS Identify Theft Affidavit, IRS Form 14039, with your return. 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. If you have already filed your 2015 tax return and it has been accepted by the IRS, you may file the IRS Identify Theft Affidavit, IRS Form 14039, with your 2016 return next year.

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.ftc.gov/idtheft/, 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. **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, (919) 716-6400, www.ncdoj.gov. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed because of law enforcement.

Massachusetts Eye and Ear
Processing Center • P.O. BOX 141578 • Austin, TX 78714

02814
TO THE PARENT OR GUARDIAN OF
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

June 16, 2016

RE: Notice of Data Security Breach

Dear Parent or Guardian of John Sample,

I write to inform you about an incident that may affect the security of some of John Sample's personal information stored in our HR system, UltiPro. We take this incident very seriously and are writing to provide you with information and access to resources so that you can better protect against the possibility of identity theft and fraud, should you feel it is appropriate to do so.

What Happened? In late April 2016, we began investigating reports of IRS tax fraud based on comments from several employees. Upon discovering anomalies in the logs of our UltiPro HR system on May 3, 2016, which we confirmed were instances of unauthorized access on May 4, 2016, we launched a full forensic investigation into the nature and scope of the intrusion. Our IT team worked with third party forensic investigators to identify those individuals whose information was affected, as well as the data that was compromised. Unfortunately, we have now confirmed that there has been a compromise of your dependent's personal information stored in our HR system. Through this compromise, between March 21 and May 4, 2016, an unauthorized individual used stolen administrator credentials to gain access to our UltiPro system and view sensitive information. We have been working diligently to investigate and to mitigate the impact of the attack since we discovered this intrusion into our system.

What Information Was Involved? We have confirmed the information involved includes your dependent's name and Client DEF 3.

What We Are Doing. We take this incident, and the security of all personal information in our system, very seriously. Mass. Eye and Ear has 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 protections and provide additional training on safeguarding the privacy and security of information in our systems. We are providing notice of this incident to you, and to certain state regulators, and will be reporting this incident to the IRS. Additionally, we are working with third-party forensic investigators to confirm the security of our network.

As an additional precaution, we are providing all affected individuals access to twenty-four (24) months of free credit monitoring and identity theft protection services through AllClear ID. Instructions on how to enroll your

dependent are included in the enclosed *Steps You Can Take To Protect Against Identity Theft And Fraud.* We encourage you to take advantage of these services by following the instructions to enroll.

What You Can Do. You can review the enclosed *Steps You Can Take To Protect Against Identity Theft And Fraud.* You can also enroll to receive the free credit monitoring and identity restoration services through AllClear ID.

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 contact our dedicated assistance line at [redacted]. Monday through Saturday, 9 a.m. to 9 p.m. ET.

The confidentiality, privacy, and security of information in our system are our highest priorities. On behalf of the executive leadership team, I want to express our sincere regret for the inconvenience and concern this incident may have caused you and your family.

Sincerely,

John Fernandez
President & CEO

STEPS YOU CAN TAKE TO PROTECT AGAINST IDENTITY THEFT AND FRAUD

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

To help you detect the possible misuse of you dependent's information, we will be providing all affected individuals access to twenty-four (24) months of free credit monitoring service through AllClear ID. The following identity protection services start on the date of this notice and you can use them at any time during the next twenty-four (24) months.

AllClear SECURE: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-285-8908, Monday through Saturday, 9 a.m. to 9 p.m. ET, 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 1-855-285-8908, Monday through Saturday, 9 a.m. to 9 p.m. ET, using the following redemption code: Redemption Code.

Please note: While SECURE is automatically available as of the date of this notice, you must call or go online to activate the additional PRO serve at no cost to you. Also, 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 dependent's account statements, and to monitor his or her credit reports, if he or she has established credit, and explanation of benefits forms for suspicious activity. Under U.S. law, individuals are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your dependent's free credit report, if he or she has established credit, 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 dependent's 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 19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

At no charge, you can also have these credit bureaus place a Fraud Alert on your dependent's file that alerts creditors to take additional steps to verify identity prior to granting credit in your dependent's name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay the ability to obtain credit while the agency verifies identity. As soon as one credit bureau confirms the Fraud Alert, the others are notified to place Fraud Alerts on your dependent's file. Should you wish to place a Fraud Alert, or should you have any questions regarding your dependent's credit report, please contact any one of the agencies listed above.

You may also place a Security Freeze on your dependent's 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 a credit report may delay, interfere with, or prevent the timely approval of any requests made for new loans, credit mortgages, employment, housing, or other services. If an individual has been a victim of identity theft, and he or she provides the credit bureau with a valid police report, it cannot charge the individual to place, list, or remove a Security Freeze. In all other cases, a credit bureau may charge 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 dependent's 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	PO Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
1-800-685-1111	1-888-397-3742	1-888-909-8872
www.equifax.com/help/credit-freeze/en_cp	www.experian.com/freeze/center.html	www.transunion.com/securityfreeze

If you receive a notice from the IRS that leads you to believe that someone may have used your dependent's information, please notify the IRS's Identity Protection Specialized Unit (IPSU) immediately at 800-908-4490 or www.irs.gov/Individuals/Identity-Protection. You will also find information at https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft. IPSU employees are available to answer questions about identity theft and resolve any tax account issues that resulted from identity theft. If your dependent files a tax return and has not yet filed his or her 2015 tax return, do so as soon as possible and file an IRS Identify Theft Affidavit, IRS Form 14039, with the return. Select Box 2A on the form. By submitting this form you are formally notifying the IRS that your dependent is a potential victim of identify fraud and you would like to mark his or her account to identify any questionable behavior. If your dependent has already filed his or her 2015 tax return and it has been accepted by the IRS, you may file the IRS Identify Theft Affidavit, IRS Form 14039, with his or her 2016 return next year.

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect your dependent, 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.ftc.gov/idtheft/, 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. **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, (919) 716-6400, www.ncdoj.gov. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed because of law enforcement.

Massachusetts Eye and Ear

To the Family of [First Name] [Last Name]
[Address Line 1]
[Address Line 2]
[City, State Zip Code]

June 16, 2016

RE: Notice of Data Security Incident

To the Family of [First Name] [Last Name]:

I write to inform you about an incident that may affect the security of some of your loved one's personal information stored in Mass. Eye and Ear's Human Resources System, UltiPro. Mass. Eye and Ear takes this incident very seriously and we are writing to provide you with information about the incident and access to resources so that you can better protect against the possible misuse of your loved one's information, should you feel it is appropriate to do so.

What Happened? In late April 2016, we began investigating reports of IRS tax fraud based on comments from several employees. Upon discovering anomalies in the logs of our UltiPro HR system on May 3, 2016, which we confirmed were instances of unauthorized access on May 4, 2016, we launched a full forensic investigation into the nature and scope of the intrusion. Our IT team worked with third party forensic investigators to identify those individuals whose information was affected, as well as the data that was compromised. Unfortunately, we have now confirmed that there has been a compromise of your loved one's personal information stored in our HR system. Through this compromise, between March 21 and May 4, 2016, an unauthorized individual used stolen administrator credentials to gain access to our UltiPro system and view sensitive information. We have been working diligently to investigate and to mitigate the impact of the attack since we discovered this intrusion into our system.

What Information Was Involved? We have confirmed the information involved in this incident includes your loved one's name and Social Security number.

What We Are Doing. We take this incident, and the security of the personal information in our system, very seriously. Mass. Eye and Ear has 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 protections and provide additional training on safeguarding the privacy and security of information in our systems. We are providing notice of this incident to you, and to certain state regulators, and will be reporting this incident to the IRS. Additionally, we are working with third-party forensic investigators to confirm the security of our network.

What You Can Do. You can review the enclosed *Steps You Can Take To Prevent Identity Theft And Fraud.*

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 contact our dedicated assistance line at (855) 285-8908, Monday through Saturday, 9 a.m. to 9 p.m. EST.

The confidentiality, privacy, and security of information in our system are our highest priorities. On behalf of the executive leadership team, I want to express our sincere regret for the inconvenience and concern this incident may have caused you.

Sincerely,

John Fernandez
President & CEO

STEPS YOU CAN TAKE TO PROTECT AGAINST IDENTITY THEFT AND FRAUD

Mass. Eye and Ear encourages everyone to remain vigilant against incidents of identity theft and financial loss by:

- **Reviewing account statements, medical bills, and health insurance statements** regularly for suspicious activity, to ensure that no one has submitted fraudulent medical claims using your loved one's name and address. Report all suspicious or fraudulent charges to your loved one's account and insurance providers. If your loved one did not receive regular Explanation of Benefits statements, you can contact your loved one's health plan and request them to send such statements following the provision of services.

- **Contacting the IRS at www.irs.gov** to request a PIN to file your taxes, so that no one can use your loved one's information to submit a fraudulent tax return.

- **There are steps you can take to protect your loved one's credit file.** Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus so long as you verify your authorization to make such a request on behalf of your loved one. To order this 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 this credit report. We recommend contacting the three credit reporting agencies listed below to discuss your particular situation and obtain specific guidance. Once you establish a relationship with the credit reporting agency and verify your authorization to make a request on behalf of your loved one, you can request a copy of your loved one's credit report. A review of the credit report will let you know of any active credit accounts that still need to be closed or any pending collection notices. Be sure to ask for all contact information on accounts currently open in your loved one's name (credit granters, collection agencies, etc.) so that you can follow through with these entities.

- **You may also request, in writing, that the credit report list the following alert:**

  "Deceased. Do not issue credit. If an application is made for credit, notify the following person(s) immediately: (list yourself, and/or another authorized relative, and/or executor/trustee of the estate—noting the relationship of any individual listed to your family member—and/or a law enforcement agency)."

  In most cases, this flag will prevent the opening of new credit accounts in your loved one's name. Contact information for the three major credit bureaus is as follows:

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	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

- **Educating yourself further** on identity theft, fraud alerts, and the steps one can take to protect against identity theft and fraud 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.

- **Reporting suspicious activity or incidents of identity theft and fraud** to local law enforcement. Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.