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

CHRISTOPHER DILENNO
DIRECT DIAL: 215.977.4059
CHRIS.DILENNO@LEWISBRISBOIS.COM

February 26, 2015

INTENDED FOR ADDRESSEE(S) ONLY

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

Re: Notice of Data Event

Dear Sir or Madam:

We represent the University of Chicago Medical Center and University of Chicago on behalf of the UChicago Biological Sciences Division's Department of Medicine; the Department is located at 5841 South Maryland Ave, MC 6092, Chicago, Illinois 60637 ("Client"). We are writing to notify you of a data security event that compromised the security of personal information of five (5) New Hampshire residents. Our Client's investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, our Client does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Security Event

On January 22, 2015, our Client learned of a security compromise of a University of Chicago Biological Sciences Division (BSD) database through an external cyber-attack. Unauthorized access was obtained to a database that contained records related to certain current and former employees, contracted employees, and students who were at one time affiliated with the Department of Medicine. All access to the database was restricted immediately, and outside forensics experts were retained to confirm the nature and scope of the unauthorized access. The security compromise was contained approximately two (2) hours after its discovery on that same day. Our forensic experts confirmed that the cyber-attack occurred on December 25, 2014. The investigation, which is ongoing, also confirmed that personal information affected by this incident includes: names, Social Security numbers, employee identification numbers, employee usernames, sex, and marital status. In addition, some affected individuals had their work and/or personal email addresses exposed. The affected database contained no bank account information or health information including that governed by state and federal law.

Notice

On February 25, 2015, notice letters were mailed to the affected New Hampshire residents in substantially the same form as the letter attached as *Exhibit A.*

Other Steps Taken and To Be Taken

Our Client takes this matter, and the security of the personal information in its care, very seriously; it has taken appropriate measures to reduce the likelihood of this type of incident from occurring in the future. In addition to providing written notice of this incident to potentially affected individuals, these individuals are being offered access to one (1) free year of credit monitoring services and identity restoration services. Our Client is also providing these individuals with information on protecting against identity theft and fraud through a confidential, toll-free hotline. The Department of Medicine also has a representative available to answer additional questions beyond those related to protecting against identity theft and fraud.

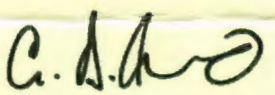
In addition to the credit monitoring and call center services provided to the affected individuals, UChicago BSD and UCMC are doing the following:

- Penetration test of internet-facing web applications;
- Exploring additional preventative and detective measures with web applications;
- Updating standards regarding the development and deployment of web applications;
- Examining the necessity for the use of Social Security numbers and eliminating the use were possible; and
- Re-evaluating the need for public access to various web applications.

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,



Christopher Dilenno of
LEWIS BRISBOIS BISGAARD & SMITH LLP

EXHIBIT A

THE UNIVERSITY OF CHICAGO
BIOLOGICAL SCIENCES

Return Mail Processing Center
P.O. Box 60
Claysburg, PA 16625

February 19, 2015

##A8255-L02-0123456 0001 00000001 **********3-DIGIT 123
SAMPLE A SAMPLE
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

Re: Notice of Data Privacy Event

Dear Sample A Sample:

We are writing to notify you of a data security compromise that may involve some of your personal information. We take the security of your personal information very seriously, and we sincerely apologize for any concern and inconvenience this may cause you. We have corrected the vulnerability and taken steps to prevent similar problems from occurring in the future. This letter contains information about the incident and our response, as well as steps we suggest you take to protect your information, including resources we are offering you. It is important that you read this letter carefully.

On January 22, 2015, we learned of a security compromise of a University of Chicago Biological Sciences Division (BSD) database through an external cyber-attack. Unauthorized access was obtained to a database that contained records related to certain current and former employees, contracted employees, and students who were at one time affiliated with the Department of Medicine. A multidisciplinary response team from Chicago Biomedicine Information Services ("CBIS"), the BSD, and University IT Services has been devoted to addressing the compromise. We immediately restricted all access to the database and retained forensics experts to confirm the nature and scope of the unauthorized access. It appears that this incident involved certain personal information, the most relevant to the protection of your identity include: your name, Social Security number, employee identification number, employee username, sex, and marital status. In addition, some individuals' work and/or personal email addresses were exposed. Your bank account information was not contained in the affected database.

Credit Monitoring

To help you protect your identity, we are offering a one-year membership in Experian's® ProtectMyID® Elite service at no charge to you. This service helps detect possible misuse of your personal information and provides you with identity protection support focused on immediate identification and resolution of identity theft.

0123456

Activate ProtectMyID Now in Three Steps

1. ENSURE **That You Enroll By: May 31, 2015** (Your code will not work after this date.)
2. VISIT the **ProtectMyID Web Site to enroll: www.protectmyid.com/enroll**
3. PROVIDE **Your Activation Code: ABCDEFGHIJKL**

(OVER PLEASE)

THE UNIVERSITY OF CHICAGO
BIOLOGICAL SCIENCES

If you have questions or need an alternative to enrolling online, please call 877-441-6943 and provide Engagement #: **PC92092.** A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
  - **Daily 3 Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax®, and TransUnion® credit reports.
  - **Internet Scan:** Alerts if your personal information is located on sites where compromised data is found, traded or sold.
  - **Change of Address:** Alerts of any changes in your mailing address.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
  - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance[1]:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.
- **Lost Wallet Protection:** If you misplace or have your wallet stolen, an agent will help you cancel your credit, debit, and medical insurance cards.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-441-6943.

Watch for Suspicious Activity

We encourage you to remain vigilant, to review your account statements regularly, and to monitor your credit reports for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

[1]Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

THE UNIVERSITY OF CHICAGO
BIOLOGICAL SCIENCES

At no charge, you can 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. Information regarding security freezes is also available from these agencies.

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

Further Information

You can further educate yourself regarding identity theft, security freezes, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. **For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us. **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. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.ftc.gov/idtheft, 1-877-ID-THEFT (877-438-4338); TTY: 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. This notice has not been delayed because of law enforcement; however, instances of known or suspected identity theft should also be reported to law enforcement.

Watch for "Phishing"

In addition to the above resources, we would like you to be watchful of "phishing" and other types of fraud that can be perpetrated. A phishing email is designed to trick you into giving access to your system or your personal data. These emails will appear to come from people or websites you trust, like your employer, vendors, and bank or credit card companies. Phishing emails often ask you to click on an internet link or an email attachment that disguises a virus or malicious software, or directly requests that you provide personal information either over the phone or through a form. If you suspect that you received a phishing email, do not click on any suspicious links or attachments contained in the email or otherwise respond to the sender. Please follow standard security procedures to report any suspicious activity.

Answers to Your Questions

We recognize that you may have questions that are not answered in this letter. We have established a confidential, toll-free hotline at Experian staffed with experts in identity fraud and protection to assist you with questions regarding the incident, this letter or Experian's identity monitoring and protection services. The hotline can be reached at 877-441-6943, Monday - Friday 6:00 AM - 6:00 PM (Pacific), and Saturday - Sunday 8:00 AM - 5:00 PM (Pacific). The call center can also direct you to a representative in the Department of Medicine who is designated to address additional questions or concerns you may have about this situation.

0123456

A8255-L02

THE UNIVERSITY OF CHICAGO
BIOLOGICAL SCIENCES

We again apologize and remain committed to the security of personal information, and have taken corrective measures to prevent this situation from recurring.

Sincerely,

Everett E. Vokes, MD
John E. Ultmann Professor
Chairman, Department of Medicine
Physician-in-Chief,
University of Chicago Medicine and Biological Sciences

Kenneth C. Goodell
Executive Administrator
Department of Medicine

A8255-L02