McDonald Hopkins
A business advisory and advocacy law firm®

RECEIVED
JUN 02 2017
CONSUMER PROTECTION

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304
P 1.248.646.5070
F 1.248.646.5075

James J. Giszczak
Direct Dial: 248.220.1354
jgiszczak@mcdonaldhopkins.com

May 26, 2017

Attorney General Michael A. Delaney
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: AU Medical Center, Inc./Augusta University – Incident Notification

Dear Attorney General Delaney:

McDonald Hopkins PLC represents AU Medical Center, Inc. ("AUMC") and Augusta University. I write to provide notification concerning an incident that may affect the security of personal information of one (1) New Hampshire resident. AUMC and Augusta University's investigation is ongoing and this notification will be supplemented with any new significant facts or findings subsequent to this submission, if any. By providing this notice, AUMC and Augusta University do not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

AUMC and Augusta University learned that a limited number of medical faculty at Augusta University were victims of a phishing attack to their email system. Upon learning of the issue, Augusta University promptly disabled the impacted email accounts and required password changes for the compromised accounts and maintained heightened monitoring of the accounts to ensure that no other suspicious activity was taking place. In addition, Augusta University commenced an investigation into the incident and retained an independent computer forensic firm to analyze the extent of any compromise to the email accounts and the security of the emails and attachments contained within them.

Since completing the forensic investigation and comprehensive manual document review, on March 29, 2017, the forensic investigation concluded that an unauthorized third party accessed members of the medical faculty email accounts containing protected health information of less than 1% of AUMC's patient population. The investigation further determined that the compromise of the email accounts occurred during a limited period of time from September 7, 2016 to September 9, 2016, but the forensic firm could not definitively conclude if information was actually accessed, viewed, downloaded or otherwise acquired by the unauthorized user.

AUMC and Augusta University confirmed that the compromised email accounts contained patient full name and either one or more of the following: address, date of birth,

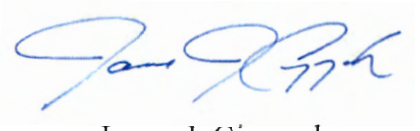
medical record number, insurance information, prescription information, diagnosis/condition, and/or treatment information. A limited number of Social Security numbers were involved.

AUMC and Augusta University wanted to make you (and the affected resident) aware of the incident and explain the steps AUMC and Augusta University are taking to help safeguard the resident against identity fraud. AUMC and Augusta University provided the New Hampshire resident with written notice of this incident commencing on May 26, 2017, in substantially the same form as the letter attached hereto. AUMC and Augusta University are offering the resident a complimentary membership with a credit monitoring and identity theft protection service. AUMC and Augusta University have advised the resident to remain vigilant in reviewing financial account statements for fraudulent or irregular activity. AUMC and Augusta University have advised the resident about the process for placing a fraud alert on their credit files, placing a security freeze, and obtaining a free credit report. The resident also has been provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

AUMC and Augusta University take its obligation to help protect personal information very seriously. AUMC and Augusta University are continually evaluating and modifying practices to enhance appropriate security and privacy measures, including ongoing cybersecurity awareness of their workforce.

Should you have any questions regarding this notification, please contact me at (248) 220-1354 or jgiszczak@mcdonaldhopkins.com.

Sincerely,



James J. Giszczak

Encl.

[redacted]

IMPORTANT INFORMATION
PLEASE READ CAREFULLY

[redacted]

Dear [redacted],

The privacy of your personal information is of the utmost importance to AU Medical Center, Inc. ("AUMC") and Augusta University. AUMC is the academic medical center affiliated with Augusta University. We are writing to provide you with important information about a recent incident involving some of your protected health information that you supplied to AUMC. We want to provide you with information regarding the incident and let you know that we continue to take significant measures to protect your information.

We learned that a limited number of our medical faculty at Augusta University were victims of a phishing attack to our email system. Phishing attacks can be emails sent to individuals appearing to be legitimate from unauthorized users requesting personally identifiable information, protected health information, or other confidential information. Upon learning of the issue, Augusta University promptly disabled the impacted email accounts and required password changes for the compromised accounts and maintained heightened monitoring of the accounts to ensure that no other suspicious activity was taking place. In addition, Augusta University simultaneously commenced an investigation into the incident and retained an independent computer forensic firm to analyze the extent of any compromise to the email accounts and the security of the emails and attachments contained within them.

Since completing our investigation and manual document review, on March 29, 2017, the investigation concluded that an unauthorized third party accessed members of our medical faculty email accounts containing your protected health information. The investigation further determined that the compromise of the email accounts occurred during a limited period of time from September 7, 2016 to September 9, 2016, but the forensic firm could not definitively conclude if your information was ***actually*** accessed, viewed, downloaded or otherwise acquired by the unauthorized user.

Further, based on the investigation conclusion, we have devoted considerable time and effort to determine what information was contained in the affected email accounts. We can confirm that the compromised email accounts contained your full name, home address, medical record number, date of birth, and Social Security number. Your medical information and financial account information was **not** contained in the compromised account.

To date, we are not aware of improper use of your information. Due to the complexity of the intrusion, however, we cannot conclusively determine whether the unauthorized user actually

acquired or viewed any of your information. Out of an abundance of caution, we wanted to make you aware of the incident.

To protect you from potential misuse of your information, we are providing you with one year of free credit monitoring and identity theft protection services. Enclosed in this letter, you will find information on enrolling in a 12-month membership of Experian's ProtectMyID® Alert, a credit monitoring and identity theft protection service, along with other precautionary measures you can take to protect your personal information, including placing a Fraud Alert, placing a Security Freeze, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis. To the extent it is helpful, we have provided steps you can take to protect your health information.

On behalf of AUMC and Augusta University, please accept our sincere apologies that this incident occurred. We are committed to maintaining the privacy of AUMC patients' information, and we continually evaluate and modify our practices to enhance appropriate security and privacy measures, including ongoing cybersecurity awareness of our workforce.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time.

Sincerely,

[redacted]

[redacted]
AU Medical Center, Inc.
Augusta University

– ADDITIONAL PRIVACY SAFEGUARDS INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

Protecting your personal information is important to AU Medical Center, Inc. and Augusta University. In response to this security incident and as a precautionary measure, we have arranged for you to enroll in Experian's® ProtectMyID® Alert for a one year period at no cost to you. This protection is provided by Experian, one of the three major nationwide credit reporting companies.

Activate Experian's® ProtectMyID Now in Three Easy Steps:

1. ENSURE that you enroll by [redacted].
2. VISIT the ProtectMyID Web Site to enroll: [redacted]
3. PROVIDE your 9-character Activation Code: [redacted]

If you have questions or need an alternative to enrolling online, please call [redacted] and provide Engagement # [redacted].

Additional Details Regarding Your 12-Month ProtectMyID Membership:

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 Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identify 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 an incident. 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:** Immediately covers certain costs including lost wages, private investigator fees, and unauthorized electronic fund transfers. (Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of 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.)

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 [redacted].

2. Placing a Fraud Alert.

Whether or not you choose to use the complimentary 12 month credit monitoring services, we recommend that you place an initial 90-day "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call

any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348
www.equifax.com
1-800-525-6285

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

TransUnion LLC
P.O. Box 2000
Chester, PA 19016
www.transunion.com
1-800-680-7289

3. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. 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
https://www.freeze.equifax.com
1-800-685-1111
1-800-349-9960 (NY residents only)

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
http://www.transunion.com/securityfreeze
1-888-909-8872

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If you live in ***North Carolina***, in addition to the FTC, the North Carolina Office of the Attorney General can also be contacted to obtain information on the steps you can take to prevent identity theft:

North Carolina Department of Justice
Office of the Attorney General
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

Instances of known or suspected identity theft should also be reported to law enforcement.