15821

October 2, 2019

Name
Address

Dear ,

We are writing to notify you of an event which included unauthorized access to your personal information in possession of Lahey Hospital & Medical Center, a member of Beth Israel Lahey Health, on or around July 25, 2019. We are prohibited by Massachusetts law from sharing any details about the incident in this letter. However, we welcome the opportunity to discuss this matter with you further. For more information about the incident and the personal information involved, please contact Dale Rice, Compliance & Privacy Manager at 781 744-9653 or by email at dale.rice@lahey.org.

We are committed to protecting your privacy and apologize for any inconvenience caused by this incident. In support of this commitment and as required by Massachusetts law, we will provide you with complimentary credit monitoring services for two (2) years through Identity Guard as described below.

Complimentary Credit Monitoring

To enroll in the program, go to the Identity Guard website at www.identityguard.com/enroll, enter this redemption code:_____ click "Submit and complete the Identity Guard enrollment form. In order to enroll, you will need to provide the following personal information:

- Mailing Address
- Phone Number
- Social Security Number
- Date of Birth
- E-mail Address
- Redemption Code

Your Rights

Under Massachusetts law you have the right to obtain any police report filed in relation 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.

You may also place a security freeze on your credit reports, free of charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware 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. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

For detailed information about how to detect and prevent identity theft, and how to request, life or remove a security freeze, please see Attachment A.

Conclusion

Protecting your privacy is extremely important to us and we apologize for any inconvenience that this incident may have caused you. Please contact me at 781 744-9653 if you have any questions regarding this matter.

Sincerely,

Dale W. Rice, BSN, RN
Compliance & Privacy Manager
Lahey Hospital & Medical Center

Attachment A

More Information about Identity Theft Prevention

We encourage you to consider the following proactive steps designed to detect and prevent financial fraud, medical identity theft or other misuse of your personal information:

Review your Credit Reports and Account Statements

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report once every 12 months by either visiting http://www.annualcreditreport.com, calling toll-free at 877-322-8228, or by completing an Annual Credit Report Request Form (found at http://www.ftc.gov/bcp/menus/consumer/credit/rights.shtm) and mailing it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

You can also purchase a copy of your credit report by contacting one of the three national credit reporting companies:

Equifax	Experian	TransUnion
(800) 685-1111	(888) 397-3742	(800) 916-8800
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 9532	P.O. Box 6790
Atlanta, GA 30374-0241	Allen, TX 75013	Fullerton, CA 92834-6790

When you receive your credit reports, review them carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personal information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to proper law enforcement authorities, including local law enforcement. You may contact your local state Attorney General's Office or the national credit reporting agencies listed above, to learn about preventing identity theft and to obtain additional information about avoiding identity theft. All U.S. residents may also contact the Federal Trade Commission ("FTC") for additional information at the following address:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
http://www.ftc.gov/idtheft/

Fraud Alerts

You should also consider placing a fraud alert to put your creditors and potential creditors on notice that you may be a victim of fraud. There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an

extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax	Experian	TransUnion
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Credit or "Security" Freezes

You have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit.

You must place your request for a freeze with each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com). To place a security freeze on your credit report, you may send a written request by regular, certified or overnight mail at the addresses below. You may also place a security freeze through each of the consumer reporting agencies' websites or over the phone, using the contact information below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-349-9960
https://www.equifax.com/personal/credit-report-services/

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

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
https://www.transunion.com/credit-freeze

In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed;

6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to remove the security freeze.

Review Your Account Statements and EOBs

Read the Explanations of Benefits (EOBs) that you receive from your medical insurance provider and other insurance companies. Make sure the health care claims submitted to your insurers by health care providers that are listed on those EOBs *actually match* the items and services that you received. Look for the name of the provider, the date of service and the service provided. If someone has stolen your medical identity, your EOBs may contain dates and services that you do not recognize.

Consider Applying for an Identity Protection PIN with the IRS

An IP PIN is a six-digit number assigned to eligible taxpayers that helps prevent the misuse of your SSN on fraudulent federal income tax returns. If you know your SSN has been compromised, or are concerned that it may have been, obtaining an IP PIN from the IRS can help prevent someone from using your SSN to submit a fraudulent tax return without you knowing in order to steal a refund check.

Important: You are currently unable to opt out once you get an IP PIN. You must use an IP PIN to confirm your identity on all federal tax returns you file this year and in subsequent tax years. If you e-file your return and your IP PIN is missing or incorrect, our system will reject your return. Filing a paper return with a missing or incorrect IP PIN delays its processing. This is for your protection so the IRS can determine it's your return.

To get your IP PIN, you must verify your identity online at http://www.irs.gov/Individuals/Get-An-Identity-Protection-PIN. You will need to have immediate access to your email account to receive a confirmation code. You will receive your IP PIN online once the IRS verifies your identity. The IRS will then send you a new IP PIN each December by postal mail. If you move, you must submit a change of address form to the IRS.

Visit the IRS's online page of FAQs for more information and to determine whether the IP PIN might be right for you at: http://www.irs.gov/Individuals/Frequently-Asked-Questions-about-the-Identity-Protection-Personal-Identification-Number-(IP-PIN)

Warnings about Email and Phishing Scams

Please be aware of scams involving emails attachments, and web links (phishing).. The following tips, although written with this particular incident in mind, reflect critical *do's and don'ts* when it comes to email and phishing scams.

Don't open emails or links from people you do not know.
Don't open and email or attachment you are not expecting
Don't open an email or attachment that offers something that is "too good to be true"
Don't open an email or attachment with a message that seems too urgent
Do check to make sure the email return address is correct and/or the message contains the right web address
Don't reply to an email if the "reply to" address does no match the address of the sender
DO stop and ask yourself if it makes sense to enter your username and password where requested
DO check your credit card and bank statements for any suspicious charges or entries.
DO check your credit reports periodically.