Boston Medical Center
HEALTH SYSTEM

To Enroll, Please Visit:

https://app.idx.us/account-creation/protect

Enrollment Code: XXX

Important Notice Regarding Security Incident

Subject: Your BMC User Account – John Doe

Dear John,

I hope this message finds you well. We are writing to inform you of a recent security incident that may have affected your BMC user account.

What Happened: On March 9, 2025, our Information Technology team detected unusual activity associated with your user account. After a thorough investigation, we determined that unauthorized access to your account occurred, and your personal information may have been viewed as a result.

What Information Was Involved: The affected information may include information within your Workday account, including:

- *Personal Information within your Workday account such as your name, address, and Social Security number. [add other data elements -under state law, BMC must be specific even if the extent is unknown - i.e., Social Security number, driver's license number, state issued identification number).*
- *Bank Account and Routing Information*
- *Any other information stored within your Workday account*

What We Are Doing/Have Done: Our team took steps to secure your account and prevent further unauthorized access. These steps include:

- *Resetting your account password*
- *Conducting a comprehensive review of our password reset guidelines and procedures*
- *Monitoring your account for suspicious access*

In addition, we are offering identity theft protection services through IDX. IDX identity protection services include 24 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

We encourage you to enroll in free IDX identity protection services by going to https://app.idx.us/account-creation/protect or calling 1-800-939-4170 and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is June 30, 2021.

While we do not have any evidence that your information has been misused, we encourage you to take full advantage of this service offering.

What You Need to Do: To protect your account, please follow these steps:

1. ***Change Your Password(s):*** *Use strong, unique passwords that you have not used before. We have already changed your BMC password.*
2. ***Monitor Your Account:*** *Keep an eye on your account activity and report any suspicious behavior to our Information Technology Security team immediately at 617-414-4500*
3. ***Enable Two-Factor Authentication:*** *If not already enabled, please activate two-factor authentication for added security on your personal accounts including banking.*

For additional information on how you can protect yourself and your information, please see the enclosure.

Our Commitment to You: We understand the seriousness of this situation and are committed to protecting your personal information.

Thank you for your understanding and prompt attention to this matter. If you have any questions or need further assistance, please do not hesitate to contact me at 617-901-0454.

Sincerely,

Lee Cullivan | Chief Information Security Officer
Boston Medical Center Health System | Cybersecurity
One Boston Medical Center Place, Boston, MA 02118
C 617-901-0454 • **E** lee.cullivan@bmc.org

Information about Identity Theft Protection

Monitor Your Accounts

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 online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax® P.O. Box 740241 Atlanta, GA 30374-0241 1-800-685-1111 www.equifax.com	Experian P.O. Box 9701 Allen, TX 75013-9701 1-888-397-3742 www.experian.com	TransUnion® P.O. Box 1000 Chester, PA 19016-1000 1-800-888-4213 www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for 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.

Credit Freeze

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) 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 access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies listed below.

Equifax P.O. Box 105788 Atlanta, GA 30348-5788 1-800-685-1111 www.equifax.com/personal/ credit-report-services	Experian P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/ freeze/center.html	TransUnion P.O. Box 2000 Chester, PA 19016-2000 1-888-909-8872 www.transunion.com/ credit-freeze

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

1. Full name, with middle initial and any suffixes;
2. Social Security number;
3. Date of birth (month, day, and year);
4. Current address and previous addresses for the past five (5) years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. Other personal information as required by the applicable credit reporting agency;

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.

Fraud Alerts

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts 1-year and is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

Equifax	Experian	TransUnion
P.O. Box 105788 Atlanta, GA 30348-5788 1-888-766-0008 www.equifax.com/personal/ credit-report-services	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/ fraud/center.html	P.O. Box 2000 Chester, PA 19016-2000 1-800-680-7289 www.transunion.com/fraud- victim-resource/place-fraud-alert

Additional Information

You can further educate yourself regarding identity theft and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC.

The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

For more information about identity theft and your tax records, we recommend that you visit the IRS Taxpayer Guide to Identity Theft at http://www.irs.gov. You may want to consider notifying the IRS that your tax records may be at risk by completing IRS Form 14039 (Identity Theft Affidavit) which can be located at http://www.irs.gov/pub/irs-pdf/f14039.pdf. You will need to send Form 14039 to the IRS along with a copy of your valid government-issued identification, such as a Social Security card, driver's license, or passport to the address on the form or by faxing to 1-855-807-5720.

Detailed below are a few things to keep in mind when filing Internal Revenue Service Form 14039:

- All documents, including your identification, must be clear and legible;
- The identity theft marker will remain on your file for a minimum of three tax cycles;
- Any returns containing your Social security number will be reviewed by the IRS for possible fraud; and,
- The marker may delay the processing of any legitimate tax returns.

You may also have the right to file or obtain a police report with your local law enforcement office if you believe you have been a victim of identity theft or fraud.

Remember to remain vigilant in reviewing your account statements, monitoring your free credit reports, and for incidents of fraud or identity theft.