Beth Israel Lahey Health
Beth Israel Deaconess Medical Center

Please Read This Important Notice

January 21, 2026

[redacted]

Dear [redacted],

We are writing to notify you of an incident that involves your protected health information. On December 19, 2025, Beth Israel Deaconess Medical Center (BIDMC) learned of an incident where a form related to your participation in a research study was inadvertently disclosed to another patient. Upon receipt, the patient alerted us and disposed of the correspondence. That said, due to the information disclosed, which included your full social security number, we are reporting this.

BIDMC takes this incident and the protection of your protected health information extremely seriously. We apologize for any inconvenience or concern this situation may cause you.

At present, we have no reason to believe that your protected health information was used for an unauthorized purpose. However, BIDMC believes that it is important for you to be fully informed of any potential risk resulting from this incident. That is why we are writing to you today. We are advising you to take a few basic steps as a precautionary measure to be extra attentive to signs of any possible misuse of your personal health information or identity.

- We recommend that you regularly review the "Explanation of Benefits" sent by your healthcare insurer. If you see any service that you believe you did not receive, please contact us at the telephone numbers listed below. You should also follow up with your healthcare insurer and healthcare provider.

- If you do not receive regular explanation of benefits statements, contact your provider or plan and request them to send such statements following the provision of services in your name or number.

- You may also want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the telephone number on the report.

- You may also request a copy of your medical records from BIDMC to serve as a baseline.

Beth Israel Lahey Health
Beth Israel Deaconess Medical Center

- Keep a copy of this notice for your records in case of future problems with your medical records.

- We are ***attaching*** a brief guide to identity theft, which includes useful resources as well as information on filing a report with the police, requesting a security freeze from the credit reporting agencies, and tips on monitoring your accounts and information for indications of identity theft.

What we are doing to protect your information:

To help protect your identity, we are offering a complimentary 24-month membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: 04/30/2026
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your **activation code**: [redacted]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (877)890-9332 by 04/30/2026. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only. *
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.

Beth Israel Lahey Health
Beth Israel Deaconess Medical Center

- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (877) 890-9332. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).
Please note that this Identity Restoration support is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

BIDMC is committed to maintaining the privacy of all protected health information and proactively takes precautions to maintain the integrity and security of that information. We follow all applicable State and Federal laws regarding the confidentiality of patient information and we take every reasonable precaution to prevent the unauthorized use and disclosure of such information. We continually test and modify systems, while aggressively enhancing practices to secure sensitive information. In this case, BIDMC has counseled the involved employee on the seriousness of this issue.

No one from BIDMC will contact you by phone, e-mail or any other method to ask you for personal information. However, please be aware that people falsely identifying themselves as BIDMC representatives might contact you claiming to offer assistance. I strongly urge you not to release any personal information in response to unsolicited inquiries.

If you wish to speak to someone at BIDMC about this notice or have questions about what to do, you may call me directly at [redacted] between 9 a.m. and 5 p.m., Monday through Friday. If I am not available to take your call, please state in your message that you are calling about this letter and I will call you back as soon as possible. Additionally, please notify me if you believe that your protected health information has been misused.

Sincerely,

[redacted]

[redacted]
AMC Director, Compliance and Privacy Officer, BIDMC
BILH Integrity and Compliance

Enclosure: BIDMC Guide to ID Theft

Beth Israel Lahey Health
Beth Israel Deaconess Medical Center

A BRIEF GUIDE TO IDENTITY THEFT RESOURCES

If you discover that someone has misused your personal information, there are several important steps you should take to protect yourself. A number of State and Federal authorities and consumer groups have prepared literature to explain the various tools and resources available to you and you can learn more by visiting their websites or contacting them at:

Federal Trade Commission 600 Pennsylvania Ave., N.W.
Washington, D.C. 20580
www.ftc.gov/idtheft

To Report Fraud:
1-(877) IDTHEFT (438-4338)
TTY: 1-866-653-4261

Office of Attorney General . Andrea Joy Campbell
One Ashburton Place
Boston, MA 02108-1518
www.mass.gov/ago

Tel.: (617) 727-2200
Consumer Hotline: (617) 727-8400

National Crime Prevention Council
2001 Jefferson Davis Highway Suite 901
Arlington, VA 22202
www.ncpc.org

Tel. (202) 466-6272

In addition, you can visit websites run by a number of government agencies and private companies to get helpful information and advice:

U.S. Department of Justice: www.usdoj.gov/criminal/fraud/websites/idtheft.html

U.S. Postal Inspection Service: https://postalinspectors.uspis.gov/

U.S. Secret Service: www.secretservice.gov/criminal.shtml

Federal Deposit Insurance Corporation: www.fdic.gov/consumers

Federal Reserve Bank of Boston: www.bos.frb.org/consumer/identity/index.htm

American Express: www.americanexpress.com/idtheftassistance/

Call for Action: http://www.callforaction.org/?cat=10

While these organizations can explain the tools available to you in detail, victims of identity theft are generally encouraged to do the following:

1. **Contact Your Banks & Credit Card Companies**: The first step in dealing with ongoing identity theft is to contact the financial institutions, banks and credit card companies that may be involved to notify them that someone has stolen your identity.

2. **Contact the Police**: If you find suspicious activity in your credit reports or you believe that your personal information has been misused, you have a right to obtain a police report. Call your local police department to file a police report. Remember to ask for a copy of the police report because creditors may request a copy of the police report before they remove errors or fraudulent transactions from your credit record.

3. **Contact a Credit Reporting Agency**: Three credit reporting agencies —Equifax, Experian and TransUnion — keep track of your credit report. When you know that someone has stolen your identity, you should call one of these agencies and report the fraud. You may contact the credit reporting agencies at the telephone numbers and addresses listed below:

Equifax
P.O. Box 740241
Atlanta, GA
30374
www.equifax.com

To obtain your credit report:
(800) 685-1111

To report fraud: (800) 525-6285

Experian
P.O. Box 9532
Allen, TX 75013
www.experian.com

To report fraud or obtain your credit report:
(888) EXPERIAN (397-3742)

TransUnion
P.O. Box 6790
Fullerton, CA 92834-6790
www.transunion.com

To obtain your credit report:
(800) 916-8800

To report fraud: (800) 680-7289

4. **Place A Restriction On Your Credit Records**: Another way to protect yourself is to restrict access to your credit report. There are two kinds of restrictions. A "fraud alert" is a temporary restriction that requires potential creditors to take additional steps to confirm your identity when someone applies for credit and attempts to open an account in your name. A "security freeze" is a stronger option created by Massachusetts law that requires credit reporting agencies to contact you directly before releasing your credit report to a potential creditor.

Fraud Alert: A fraud alert is a notice that the credit reporting agencies attach to your credit report that requires all potential creditors to use what the law refers to as "reasonable policies and procedures" to verify your identity before issuing credit in your name. A fraud alert lasts for 90 days and you can initiate an alert by calling one of the credit reporting agencies listed above (Equifax, Experian or TransUnion).
You are likely to speak with an automated call attendant, so we recommend that you follow up with a written request. You only need to contact one of the three agencies to place an alert. The agency you call is required to contact the other two. As a result, all three agencies should send you a letter confirming the fraud alert and letting you know how to get a free copy of your credit report. If you do not receive a confirmation from one or more of the agencies, you should contact that company directly to place a fraud alert. 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.

Security Freeze: Placing a security freeze on your credit file will tell the credit reporting agencies to contact you before allowing anyone to access your credit report. You may place or remove a security freeze at no cost. This means that potential creditors will not be able to get access to your credit report — for example, to open new accounts or obtain loans — unless you temporarily lift the freeze. When you place a security freeze, the credit reporting agency that you contact will provide you with a personal identification number or password to use if you wish to release your credit information to a specific person or financial institution or when you remove the security freeze from the credit file. Please note that because a security freeze adds an additional layer of security, it may delay your ability to obtain credit while the security freeze is in effect.

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number, date of birth (month, day and year); current address and previous addresses for the past two years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies.

Keep Your Eyes Open for Potential Identity Theft: Even if you do not find any suspicious activity on initial credit reports, the FTC recommends that you check your credit reports periodically. Victim information sometimes is held for later use or shared among a group of identity thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.