The Framingham Heart Study

A Project of the National Heart, Lung, and Blood Institute and Boston University

<Date>

<Recipient Address>

Dear <Insert Recipient Name>:

The Framingham Heart Study at Boston University and the National Heart, Lung, and Blood Institute (NHLBI) are writing to inform you of an incident involving your personal information related to your participation in the Framingham Heart Study. NHLBI, a component of the National Institutes of Health, is the federal agency that directs the Framingham Heart Study, and Boston University is an NIH contractor that operates the Framingham Heart Study.

The incident involved a security vulnerability that resulted in an unauthorized party accessing study information on the Framingham Heart Study's server system, which included your personal information. At this time, we do not have any knowledge that your personal information has been used for any unauthorized purpose. We are sending you this letter so that you can understand more about this incident, how we are addressing it, and additional steps you can take to further protect your privacy.

What Happened

On September 8, 2024, the Framingham Heart Study became aware of unusual activity on a computer server used by the study and began actively investigating this incident. We isolated the server to prevent further unauthorized activity and applied patches to the protected server environment to address the vulnerability. However, cyber-attackers were able to access the protected server environment and download files containing unencrypted study information before the system could be isolated. This unencrypted information included your personal information.

What Information Was Involved

Based on our investigation, your personal information was involved in the files accessed in this incident. The information included your Social Security number. It may have also included your name, address, date of birth, telephone number, email address, sex, race, ethnicity, self-reported broad income and occupational categories, signature, and medical information.

What We Are Doing

The Framingham Heart Study at Boston University and NHLBI are actively investigating the incident and have notified the appropriate law enforcement agencies. In addition, we will be hosting an online meeting to discuss any concerns you may have. We will provide you with those details in the coming days.

What Can You Do

At this time, we are not aware of any reports of identity fraud or improper use of information as a direct result of this incident. The Federal Trade Commission recommends that you monitor your credit following any data incident involving your Social Security number. Therefore, Boston University is making available to you a free 24-month membership in a credit monitoring service, Experian IdentityWorks^{SM}, to help you protect your personal information. This service will provide you with alerts of key changes and suspicious activities on your credit reports and proactive fraud assistance. You must enroll by **03/02/2025**. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. Experian IdentityWorks^{SM} is free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and Experian IdentityWorks^{SM}, including instructions on how to activate your complimentary membership, please review the enclosed documents.

You may also take advantage of the free annual credit report available from each credit reporting agency by visiting www.annualcreditreport.com. You have the right to obtain such a free report annually, from each of the three major credit reporting bureaus. If you detect any unauthorized or suspicious activity in any of your accounts, contact the issuing company immediately. If you are victim of identity theft—meaning that your personal identifying information was used to pose as you, harass you, or obtain identification containing your personal information or anything else of value—you have the right to file your own police report and obtain a copy of that report. If you find that your information is being used without your authorization, contact your local police department.

The Framingham Heart Study, Boston University, and NHLBI take your privacy and information security very seriously. We are taking steps to prevent any similar events in the future, including working with law enforcement as necessary, and will provide you with updates as needed.

We would like to express our deepest appreciation for your years of voluntary participation in the Framingham Heart Study. If you have any additional questions or concerns, please call us at **888-458-9812**.

Sincerely,

Drs. Joanne Murabito and George O'Connor

MPIs, Framingham Heart Study Center
Boston University Chobanian & Avedisian School of Medicine

What are the steps I should take to reduce my risk of identity theft?

1. **Monitor your financial statements and credit reports for unauthorized activity.**
   Contact your financial institution to determine whether your accounts should be closed. Immediately report any suspicious or unusual activity on your accounts.

   Request a free credit report at www.AnnualCreditReport.com or by calling 1-877-322-8228. You are entitled by law to obtain one free credit report per year from each of the three major credit bureaus -- Equifax, Experian, and Transunion -- for a total of three reports every year.

2. **Place a fraud alert on your credit reports.**
   Consider placing an *initial fraud alert* with the three major credit bureaus noted above. A fraud alert stays in your file for at least 90 days and can make it more difficult for someone to get credit in your name because it warns creditors to follow certain procedures to protect you. Please note, however, that these additional safeguards may also delay your own applications for new credit. You may place a fraud alert in your file by calling just one of the three nationwide consumer credit reporting companies. As soon as that agency processes your fraud alert, it will notify the other two, which then will a place fraud alerts in their files. Placing a fraud alert entitles you to free copies of your credit reports.

   Equifax: 1-800-525-6285; www.equifax.com
   Experian: 1-888-EXPERIAN (397-3742); www.experian.com
   TransUnion: 1-800-680-7289; www.transunion.com

   Deployed members of the U.S. Military should consider placing an active duty alert on their credit file. Such active duty alerts serve a similar function as initial fraud alerts, causing creditors to be more cautious in extending new credit. However, unlike initial fraud alerts, active duty alerts last for one year instead of 90 days. However, active duty alerts do not entitle you to a free credit report, so after filing this alert, you should also request a free credit report (as noted above).

3. **Review Federal Trade Commission (FTC) Resources.**
   Review resources provided on the FTC identity theft website, www.ftc.gov/idtheft. The FTC maintains a variety of consumer publications providing comprehensive information about breaches and identity theft.

What should I do if I think I am the victim of identity theft?

If you discover unauthorized activity on your accounts or credit reports and feel that you are the victim of identity theft, you should take the following steps in addition to those above.

1. **File a complaint with the Federal Trade Commission (FTC).**

   By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials across the nation track down identity thieves and stop them. The FTC can refer victims' complaints to other government agencies and companies for further action, as well as investigate companies for violations of laws the agency enforces.

   You can file a complaint with the FTC online by following the "Report ID Theft" link at the top of the FTC identity theft website, www.ftc,gov/idtheft; or call the FTC's Identity Theft Hotline, toll-free: 1-877-ID-THEFT (438-4338); TTY: 1-866-653-4261; or write Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

   Be sure to call the Hotline to update your complaint if you have any additional information or problems.

2. **File a report with your local police or the police in the community where the identity theft took place.**

   File a ***Theft*** or ***Miscellaneous Incident*** report with your local police and remember to get a copy of the police report or at the very least, the number of the report. It can assist with creditors who need proof of the crime.

3. **File an extended fraud alert.**

   You may also contact the one of the three credit reporting agencies above to place an ***extended fraud alert*** in your credit reports. An extended fraud alert will remain on your files for seven years. If you ask for an extended alert, in addition to proof of your identity, you will have to provide an identity theft report. An identity theft report includes a copy of a report you have filed with a federal, state, or local law enforcement agency. For more detailed information about the identity theft report, visit www.ftc.gov/idtheft.

To help protect your identity, we are offering a **complimentary** two-year membership of Experian IdentityWorks℠. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Identity Now in Three Easy Steps

1. ENROLL by: **03/02/2025** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: **https://www.experianidworks.com/3bcredit**
3. PROVIDE the **Activation Code**: **[Residency state specific – Ken please link]**

If you have questions about the product or need assistance with identity restoration, please contact Experian's customer care team at 877-288-8057. Be prepared to provide engagement number **B136034** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS IDENTITY MEMBERSHIP:

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

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at https://www.experianidworks.com/3bcredit Same as above?

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information.
If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. 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 from the date of the incident (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 Identity Restoration 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.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

* 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.