NAVAL CONTINUING CARE
RETIREMENT FOUNDATION, INC.

Return Processing Center:
PO Box 173071 | Milwaukee, WI 53217

<<First Name>><<Last Name>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>> <<Date>>
<<Country>>

NOTICE OF DATA PRIVACY <<HEADER>>

Dear <<First Name>><<Last Name>>:

Naval Continuing Care Retirement Foundation, Inc. d/b/a Fleet Landing ("Fleet Landing"), takes privacy and security very seriously. As part of that commitment, we are writing to notify you of a data privacy incident involving your protected health information. This notice explains the incident, outlines the steps Fleet Landing has taken to address it, and provides steps you can take to help protect your personal information. We are also offering the opportunity to enroll in complimentary credit monitoring and identity protection services.

What Happened: On September 12, 2024, we discovered suspicious activity on our network. Upon discovery, we took immediate action to secure our systems and we partnered with cyber incident response professionals to investigate the incident. After a thorough investigation, we learned that an unauthorized actor gained access to our network between September 11, 2024 and September 12, 2024 and accessed or acquired certain data from our network. As a result, we underwent a comprehensive and detailed review of the impacted data to identify what information was involved and to whom that information belonged. On September 11, 2025, we determined that some of your protected health information was included in the data set.

What Information Was Involved: Our review of the files determined your first and last name, in combination with your <<data elements>> were present within certain files within the data set.

What We Are Doing: Upon learning of the incident, we took immediate steps to address it, including securing our systems and taking parts of our network offline. We partnered with cyber incident response professionals and notified federal law enforcement and the Department of Health and Human Services, Office of Civil Rights.

As an added protection, we are offering <<CM Duration>> months of complimentary credit monitoring and identity protection services through HaystackID. Instructions for how to enroll in these services are enclosed.

What You Can Do: As a general matter, it is good practice to be vigilant against incidents of identity theft and fraud, from any source, by reviewing your credit reports and account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, promptly contact the financial institution or company. You may also file a report with law enforcement, your state attorney general, and/or the Federal Trade Commission. Please refer to the enclosed "*Steps You Can Take to Help Protect Your* Information" for additional resources you may take advantage of to protect against fraud and identity theft, should you find it appropriate to do so.

For More Information: Should you have any questions or concerns please contact our dedicated assistance line provided by HaystackID, at 877-323-4120 (toll free), during the hours of 8:00 am to 11:00 pm Eastern time, Monday through Friday, and 9:00 am to 6:00 pm Eastern time Saturday (excluding U.S. national holidays). Please know that the security of your information is of the utmost importance to us. We remain committed to safeguarding the trust you've placed in us and are deeply grateful for your continued support during this time.

Sincerely,

Naval Continuing Care Retirement Foundation, Inc. d/b/a Fleet Landing

Enclosure: *Steps You Can Take to Help Protect Your Information*

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Credit Monitoring Enrollment Instructions:

To enroll in the free credit monitoring services noted above, please log on to the following and follow the instructions provided. **https://app.identitydefense.com/enrollment/activate/FL**

When prompted please provide the following unique code to receive services: **<<Enrollment Code>**

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Monitor Your Accounts and Credit Reports:

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors.

Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

Fraud Alerts:

You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, 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 lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

Credit Freeze:

As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you should provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com **TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016-2000 **TransUnion Credit Freeze** P.O. Box 160 Woodlyn, PA 19094	**Experian** 1-888-397-3742 www.experian.com **Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013 **Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-298-0045 www.equifax.com **Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069 **Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them.

The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at 400 6th Street NW, Washington, D.C. 20001; 1-202-727-3400; and oag.dc.gov.

For Iowa residents, the Iowa Attorney General may be contacted at 1305 E. Walnut Street, Des Moise, IA 50419; 1-515-281-5164; and iowaattorneygeneral.gov.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St, Paul Place, Baltimore, MD 21202; 1-410-576-6300; and marylandattorneygeneral.gov.

For Massachusetts residents, the Massachusetts Attorney General may be contacted at 1 Ashburton Place, 20th Floor, Boston, MA 02108; 1-617-727-8400 or 1-617-727-2200; and www.mass.gov/orgs/office-of-the-attorney-general.

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Oregon residents, the Oregon Attorney General may be contacted at Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301-4096; 1-877-877-9392; and https://doj.state.or.us/consumer-protection/.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. No Rhode Island residents had their data impacted by this incident.