

NOTICE OF DATA EVENT

January 26, 2026 – Community Health Northwest Florida (“CHNF”) is providing notice of a data event that may have impacted the security of certain individuals’ information. While CHNF is unaware of any misuse of individuals’ information as a result of this event, CHNF is providing individuals with details about the event, its response to the event, and resources available to help individuals protect against the potential misuse of their information, should they wish to do so.

What Happened? On December 24, 2024, CHNF became aware of suspicious activity within its network environment. Upon becoming aware of this, CHNF immediately took steps to secure its network. Additionally, CHNF promptly engaged third-party cybersecurity specialists to assist with its response and to conduct a comprehensive forensic investigation into the nature and scope of the issue. Through this investigation, it was determined that an unauthorized party had gained access to CHNF’s network and, during that time, accessed certain files stored on some of those systems. Based on those findings, CHNF began a comprehensive and time-intensive review of the potentially impacted information, with the assistance of an outside data mining team, to identify the specific individuals and the type of data at risk. CHNF finalized the list of affected individuals on January 19, 2026, and then moved expeditiously to mail notice letters to individuals for whom address information was available.

What Information Was Involved? The impacted information varied by individuals but included names, dates of birth, Social Security numbers, driver’s license or state identification card numbers, financial account numbers, credit or debit card numbers, patient identification and medical record numbers, medical information, and health insurance information.

What CHNF Is Doing. CHNF is committed to ensuring the security and privacy of all personal information in its control. Upon becoming aware of the event, CHNF moved quickly to promptly investigate and respond to the event. Specifically, CHNF took steps to secure its systems and remediate all impacted systems and is implementing additional technical safeguards, enhanced security measures, and updated policies and procedures to mitigate against the risk of future issues. CHNF offered at least 12 months of complimentary credit monitoring and identity theft restoration services to all individuals to help protect their identity along with resources and further information on how individuals can protect against identity theft and fraud.

How Will Individuals Know If They Are Affected By This Data Event? CHNF is mailing a notice letter to individuals whose information was determined to be in the affected files and for whom a valid mailing address is available. If an individual does not receive a letter but would like to know if they are affected, they may call CHNF’s dedicated assistance line, detailed below.

Whom Should Individuals Contact For More Information? If individuals have questions or would like additional information, they may call CHNF’s dedicated assistance line at 1-833-580-0425 between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday. This excludes all major U.S. holidays.

What You Can Do. CHNF encourages individuals to remain vigilant against incidents of identity theft and fraud by reviewing their account statements, explanation of benefits forms, and monitoring their free credit reports for suspicious activity and to detect errors. Under U.S. law individuals are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report, place a fraud alert, or a security freeze. Contact information for the credit bureaus is below.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that 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 seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers 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 the consumer’s 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 to take control over who gets access to the personal and financial information in your credit report 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 security freeze, you may need to provide the following information, depending on whether the request is made online, by phone, or by mail:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); 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 a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. 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 and your state Attorney General. This notice has not been delayed by law enforcement.