



Sean B. Hoar, Partner & Chair
Cybersecurity & Data Privacy Team
4800 SW Meadows Road, Suite 300
Lake Oswego, OR 97035
shoar@constangy.com
Mobile: 503.459.7707

Emergency: BreachResponse@constangy.com
Hotline: 877-382-2724 (877-DTA-BRCH)

June 13, 2025

VIA ONLINE SUBMISSION

Re: Notification of Data Security Incident

To Whom It May Concern:

Constangy, Brooks, Smith & Prophete, LLP represents Warm Springs Medical Center (“Warm Springs”), in conjunction with their response to the Nationwide Recovery Services, Inc. incident discussed below. The purpose of this letter is to notify you of the impact to Nebraska residents in accordance with Nebraska’s data breach notification statute.

1. Nature of the Security Incident

Nationwide Recovery Services, Inc. (“NRS”) provides debt collection services for entities, including Warm Springs. On July 14, 2024, NRS notified Warm Springs of a data security event that disrupted its operations. NRS stated that they engaged cybersecurity specialists to assist with their investigation and reported the incident to federal law enforcement. On February 7, 2025, NRS notified Warm Springs that their investigation revealed unauthorized access to the NRS network between July 5 and July 11, 2024. At that time, NRS stated that they would notify affected persons about the incident on behalf of Warm Springs. On April 3, 2025, NRS notified Warm Springs that they changed their decision and would not be notifying anyone affected by the incident.

Warm Springs then worked to identify all individuals whose personal information was shared with NRS and sufficient contact information for the purpose of notifying them about the incident. That process was completed on June 3, 2025.

2. Number of Affected Nebraska Residents & Information Involved

The incident involved personal information for approximately two Nebraska residents. The information involved in the incident for affected Nebraska residents may differ depending on the individual but may include name, Social Security number, and date of birth.

3. Notification to Affected Individuals

On June 13, 2025 notification letters were sent to affected Nebraska residents by USPS First Class Mail.

The notification letter provides resources and steps individuals can take to help protect their information. The notification letter also offers individuals the opportunity to enroll in 12 months of complimentary identity protection services through IDX.

IDX will also support a call center for 90 days to answer questions and assist with enrollment. A sample notification letter is enclosed.

4. Measures Taken to Address the Incident

Upon identifying this incident, in addition to taking the steps described above, Warm Springs took steps to learn more information from NRS regarding what happened and what information could have been affected. Warm Springs notified the potentially affected individuals and provided them with steps they can take to protect their personal information, including providing them with information about how to contact them to answer questions about the incident, address related concerns, and assist with enrolling in the credit monitoring services.

5. Contact Information

If you have any questions or need additional information regarding this incident, please do not hesitate to contact us at shoar@constangy.com or bswanson@constangy.com.

Sincerely,



Sean B. Hoar of
Constangy, Brooks, Smith & Prophete LLP

Cc. Brett Swanson, Associate
Constangy, Brooks, Smith & Prophete, LLP

Encl.: Sample Notification Letter

 WARM
SPRINGS
medical center
Large enough to serve...Small enough to care
P.O. Box 989728
West Sacramento, CA 95798-9728

Enrollment Code: <<ENROLLMENT>>

To Enroll, Scan the QR Code Below:



Or Visit:

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

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

June 13, 2025

Subject: Notice of Data <<Variable Text 2: Security Incident/Breach>>

Dear <<First Name>> <<Last Name>>,

Warm Springs Medical Center (“Warm Springs”) is writing to inform you of a data security incident experienced by Nationwide Recovery Services, Inc. (“NRS”) that may have affected your personal information. NRS provides debt collection services for entities, including Warm Springs. Please read this letter carefully as it contains details about the incident and resources you can utilize to protect your information, including instructions for enrolling in complimentary credit monitoring and identity theft protection services.

What Happened? On July 14, 2024, NRS notified us of a data security event that disrupted its operations. NRS stated that they engaged cybersecurity specialists to assist with their investigation and reported the incident to federal law enforcement. On February 7, 2025, NRS notified us that their investigation revealed unauthorized access to the NRS network between July 5 and July 11, 2024. At that time, NRS stated that they would notify affected persons about the incident on behalf of Warm Springs. On April 3, 2025, NRS notified Warm Springs that they changed their decision and would not be notifying anyone affected by the incident. On April 7, 2025, we determined that some of your information may have been acquired without authorization during the incident.

What Information Was Involved? The information involved may include your name and <<Variable Text 1: Data Elements>>.

What We Are Doing. We are providing you with access to <<12/24>> months of credit monitoring, dark web monitoring, a \$1 million identity fraud loss reimbursement insurance policy, and fully managed identity theft recovery services through IDX. You have until September 13, 2025, to enroll in the services offered at no charge to you.

What You Can Do. You can follow the recommendations on the following page to help protect your personal information. You can also enroll in the identity protection services, which are offered at no cost to you by calling 1-800-939-4170, going to <https://app.idx.us/account-creation/protect>, or scanning the QR image and using the Enrollment Code provided above.

Warm Springs Medical Center
5995 Spring Street
Warm Springs, Georgia 31830

For More Information. If you have questions about this letter or need assistance, please call the dedicated team at IDX at 1-800-939-4170. IDX representatives are available Monday through Friday from 9:00 am – 9:00 pm Eastern Time. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

Sincerely,

Warm Springs Medical Center
5995 Spring Street
Warm Springs, GA 31830

Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC). You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the FTC is as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

Equifax, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, www.equifax.com.

Experian, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com.

TransUnion, P.O. Box 2000, Chester, PA 19016, 833-799-5355, www.transunion.com/get-credit-report.

Fraud Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary proof. An extended fraud alert is also free and will stay on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>. Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment.

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit.

You must separately place a security freeze on your credit file with each credit reporting agency. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the FTC identified above. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps

the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state attorney general about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the attorney general in your state.

Additional information:

California: California Attorney General can be reached at: 1300 "I" Street, Sacramento, CA 95814-2919; 800-952-5225; <http://oag.ca.gov/>

Maine: Maine Attorney General can be reached at: 6 State House Station Augusta, ME 04333; 207-626-8800; <https://www.maine.gov/ag/>

Maryland: Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us

North Carolina: North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov

New York: New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005; 212-416-8433; <https://ag.ny.gov/>

Oregon: Oregon Office of the Attorney General can be reached at: Oregon Department of Justice, 1162 Court St. NE, Salem, OR, 97301, 1-877-877-9392, www.doj.state.or.us

Texas: Texas Attorney General can be reached at: 300 W. 15th Street, Austin, Texas 78701; 800-621-0508; texasattorneygeneral.gov/consumer-protection/

Vermont: Vermont Attorney General's Office can be reached at: 109 State Street, Montpelier, VT 05609; 802-828-3171; ago.info@vermont.gov