Hamilton County Government
Risk Management
Attention: Angela M. Duncan, RHIA, CHPS
HIPAA Privacy Officer
317 Oak Street
Chattanooga, TN 37403

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

June 16, 2025

NRS Data Breach Update

Dear Affected Individual,

What Happened
As we previously made you aware in our letter to you dated April 14, 2025, Nationwide Recovery Service ("NRS") is a business associate of Hamilton County Government ("HCG") providing debt collection services for delinquent accounts for various departments, offices and organizational components of HCG. On July 14, 2024, HCG received an email from NRS with an attached letter. The letter confirmed NRS had suffered a cybersecurity event that was reported to federal law enforcement.

On Monday, February 24, 2025, the Hamilton County Attorney's Office received a letter via U.S. Mail from NRS supplementing their July 14, 2024, letter. The letter stated that NRS's investigation recently found that there was unauthorized access to the NRS network between July 5, 2024, and July 11, 2024, and that certain files and folders were copied from the system.

What Information Was Involved
NRS determined that the compromised information potentially included names, addresses, Social Security numbers, dates of birth, financial account information and/or medical related information, among other information provided to NRS by HCG.

Corrective Actions
NRS took the following corrective actions after the event to safeguard their environment:

- Network Segmentation: NRS implemented additional segregation of all offices and cloud server networks from each other.
- Access Control and Identity Management: Network users are required to access via VPN with Domain authentication and multi-factor authentication ("MFA") to access any NRS resources; role-based access control ("RBAC") to segment data access according to job roles or required permissions; enforcement of a Fine-Grained Password Policy ("FGPP"), allowing administrators to set different password and account lockout policies for specific groups of users within a domain; Local Administrator Password Solution ("LAPS") to manage local administrator passwords for domain-joined computers in Active Directory. NRS conducts audits on a daily basis when a local user is being added to device; NRS audits weekly domain administrator access; and NRS audits monthly for domain user rights.
- Data Segmentation and Classification: data is classified based on sensitivity and policy restrictions are in place to ensure the minimum as necessary policy is followed

- Micro-Segmentation: implementation of fine-grained policies within individual workloads or applications on all NRS firewalls. NRS also utilizes firewalls and Intrusion Detection/Prevention Systems ("IDS/IPS") between segments to filter traffic, monitor for suspicious activity, and enforce segmentation policies. This setup includes rules to block unauthorized lateral movement within the network.
- More Regular Audits and Monitoring: NRS regularly conduct audits and monitor user-based permissions and network traffic, including Datto log monitoring and segmentation reviews, to detect any anomalies or unauthorized activity. The NRS team checks Kaseya Datto RMM and EDR for any alerts on a daily basis. Additionally, the NRS team reviews on a weekly basis that all devices to ensure Kaseya Datto RMM and AntiVirus/EDR is installed and operating properly.
- Patching and Vulnerability and Remediation: deployment and integration of Datto RMM/EDR for patching and vulnerability management. In addition to Datto, NRS leverages RocketCyber to remediate critical vulnerabilities with 24/7 monitoring and containment functionality.
- Backup and Recovery: Restructuring of Veeam Enterprise Backup and replication, including nightly backups to a backup storage server, followed by an immutable backup that sends the backups offsite storage.

What HCG is Doing
HCG is offering identity theft protection services through IDX, data breach and recovery services expert, for qualified individuals affected by the NRS Data Breach. All affected HCG patients are qualified. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do
We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 800-939-4170, going to https://app.idx.us/account-creation/protect, or scanning the QR image. **You will need to call the HCG Privacy Officer at phone number 1-833-484-8671 to obtain an Enrollment Code.** Please note the deadline to enroll is September 30, 2025.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives can answer questions or concerns you may have regarding protection of your personal information.

For More Information
You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Please call 800-939-4170 or go to https://app.idx.us/account-creation/protect for assistance or for any additional questions you may have. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. **You will need to call the HCG Privacy Officer at phone number 1-833-484-8671 to obtain an Enrollment Code.**

Sincerely,

Hamilton County Government

(Enclosure)

Recommended Steps to Help Protect Your Information

Please Note: You will need to call the HCG Privacy Officer at phone number 1-833-484-8671 to obtain an Enrollment Code.

1. **Website and Enrollment.** Scan the QR image or go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code. Call

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.
Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** https://www.marylandattorneygeneral.gov, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.