Ruffolo, Hooper & Associates, MD, PA
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

<Name>
<Address>
<City>, <State> <Zip>

May 19, 2025

Dear <Name>:

Ruffolo, Hooper & Associates, MD, PA ("RHA") is writing to notify you of an incident experienced by Nationwide Recovery Services ("NRS"), a third-party vendor utilized by RHA, that may have involved some of your personal information as described below. Importantly, this incident was limited to NRS systems, and no RHA systems were impacted in any way.

What Happened: On February 7, 2025, we received notification advising that NRS experienced an incident which may have impacted information related to individuals associated with RHA. According to NRS, they discovered suspicious system activity in July 2024, and following investigation, determined there was unauthorized access to the NRS network between July 5, 2024 and July 11, 2024 which resulted in the acquisition of certain data maintained by NRS. Upon discovery of the NRS incident and potential impact to RHA, we worked to obtain additional information regarding the incident and potential scope of impact, including the identification of individuals potentially affected so that you could be provided with notice. On or around April 3, 2025, NRS advised that they would not be providing individual notification, and we worked to engage the appropriate resources to provide this notice.

What Information Was Involved: Based on the information provided by NRS, we understand that that the types of information potentially impacted may include your first and last name in combination with address, Social Security number, date of birth, gender, facility name, date of service, insurance carrier name, and/or insurance policy number.

What We Are Doing: Upon learning of this incident, we took steps to obtain additional information from NRS regarding the incident and steps taken by NRS in response to this matter. NRS has advised that additional cybersecurity measures have been implemented to prevent a similar incident in the future and that are reviewing their existing security policies.

As an additional safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring and identity protection services for a period of 12 months.

What You Can Do: In addition to enrolling in the complimentary credit monitoring service detailed within, we recommend that you 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. If you discover any suspicious or unusual activity on your accounts, please promptly contact the financial institution or company with which the account is maintained. We have provided additional information in the attached Reference Guide, which contains more information about steps you can take to help protect yourself against fraud and identity theft.

For More Information: Should you have any questions or concerns, please contact our dedicated assistance line at <Contact Number>, between 8 am - 8 pm Eastern Time, Monday through Friday excluding U.S. holidays. RHA may also be contacted by mail at P.O. Box 918377, Orlando, FL 32891.

We sincerely appreciate your understanding in this matter.

Sincerely,

RHA

REFERENCE GUIDE

Enroll in Credit Monitoring and Identity Protection Services

To enroll in Credit Monitoring services at no charge, please log on to **https://bfs.cyberscout.com/activate** and follow the instructions provided. When prompted please provide the following unique code to receive services: **<Code>**. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services

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

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. Report any questionable charges promptly to the financial institution or company with which the account is maintained.

Order Your Free Credit Report

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 toll-free at 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. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you have questions or notice incorrect information, contact the credit reporting bureau by calling the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected.

Place a Fraud Alert on Your Credit File

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.

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

Security Freezes

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 place a security freeze on your credit report, you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity.

To request a credit freeze, you will need to 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 credit freeze, please contact the three credit reporting bureaus listed below:

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

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than 5 business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

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.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and https://www.marylandattorneygeneral.gov.

For 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: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from violators. 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. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

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 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. There are [#] Rhode Island residents impacted by this incident.

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 400 6th Street NW, Washington, D.C. 20001; 202-442-9828, and https://oag.dc.gov/consumer-protection.