Amicus Solutions, Inc.
c/o Cyberscout
PO Box 245
Bellmawr, NJ 08099

USBFS3768 - T3 P1 - 916

[redacted]

0102000916

June 3, 2026

RE: Notice of Security Incident

Dear [redacted],

Amicus Solutions, Inc. d/b/a Fedora Solutions ("Amicus," "we," or "us") provides revenue cycle management services for certain medical practices managed by OneOncology, LLC ("OneOncology") including New York Cancer and Blood Specialists ("NYCBS"). We are writing to provide you with notice of a recent security incident that occurred at Amicus which impacted some of your information and to inform you about steps you may take to help protect your information. We are actively investigating this security incident. Importantly, this incident did not impact NYCBS's or OneOncology's network or systems.

What Happened? On or around April 2, 2026, Amicus leadership became aware of suspicious activity within the company's IT environment (the "Incident") that is believed to have occurred between February 2 and February 18, 2026. After becoming aware of the Incident, we initiated our incident response protocols, notified law enforcement and began taking measures to assess and contain the unauthorized activity. As part of our response process, we initiated a comprehensive investigation into the matter with the support of industry leading third-party specialists. While our investigation remains ongoing, Amicus determined that some of your protected health information ("PHI") or personally identifiable information ("PII") was obtained by an unauthorized, unknown third-party actor and that the actor posted this information on their public website. We are providing you with this notification so that you may take steps to protect your information. **Based on Amicus' investigation and remediation efforts to date, there is no evidence of identity theft or fraud related to your information as a result of this matter**.

What Information Was Involved? Our investigation into the Incident remains ongoing. To date, we have determined that certain categories of personal information were copied by a third party, including: your first and last name, email address, phone number, date of birth, gender, Social Security number, medical data and health insurance information. Again, at this time, we have no evidence of identity theft or fraud related to your PHI or PII as a result of the Incident.

What We Are Doing. Amicus takes its responsibility to protect all data entrusted to it very seriously. As part of our ongoing commitment to the privacy and security of PHI and PII in our care, we have implemented additional safeguards to further secure our systems and the information contained therein. We are also consulting with federal law enforcement and actively working to have the unauthorized actor's public website taken down. To help further protect your information, we are offering you twenty-four (24) months of free identity protection services. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll for the free 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: [redacted].

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

10102000916000

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.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your financial account statements, Explanation of Benefits (EOB) documents and credit reports for any anomalies.

For More Information. In addition to the information provided in this letter, we have also enclosed an attachment with additional information and resources. If you have additional questions, please call the assistance line at 1-800-405-6108, Monday through Friday from 8:00 a.m. to 8:00 p.m. Eastern Time, excluding major U.S. holidays. Please have this letter ready if you call.

Sincerely,
Amicus Solutions, Inc.

ADDITIONAL RESOURCES

The following provides additional information and actions that you can consider taking to help protect your information. You may also contact the U.S. Federal Trade Commission ("FTC"), the credit reporting agencies, or your state's regulatory authority to obtain additional information about avoiding identity theft, including information about fraud alerts and security freezes, as further detailed below. Contact Information for the Federal Trade Commission and credit reporting agencies is set forth below:

The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

Credit Reporting Agencies

Equifax	**Experian**	**TransUnion**
PO Box 740241	PO Box 4500	PO Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Order Your Free Annual Credit Report. You can order your free annual credit report online at www.annualcreditreport.com. by phone (toll free) at 877-322-8228, or by mail by submitting a completed Annual Credit Report Request Form to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can download a copy of the request form on the FTC website: www.ftc.gov. You can also visit the Consumer Financial Protection Bureau's website for more information on how you can obtain your credit report for free: www.consumerfinance.gov. Once you receive your credit reports, review them carefully for any discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting agency.

Review Your Accounts and Report Unauthorized Activity. We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the FTC. Carefully review your credit reports and bank, credit card, and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of suspicious activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company. You may also consider filing or obtaining a police report.

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from potential identity theft, you may consider placing a fraud alert on your credit file. A fraud alert is intended to make it more difficult for someone to open a new credit account in your name. A fraud alert indicates to an entity requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the alert notifies the entity to take steps to verify your identity. You may contact one of the credit reporting agencies listed above for assistance.

Consider Placing a Security Freeze on Your Credit File. You also may consider implementing a security freeze (also called a "credit freeze"). Placing a freeze on your credit report restricts access to your credit report and will prevent lenders and others from accessing your credit report entirely. This means you (or others) will not be able to open a new credit account while the freeze is in place. You can temporarily lift the credit freeze if you need to apply for new credit. With a security freeze in place, you may be required to take special steps when you wish to apply for any type of credit. You may contact one of the credit reporting agencies listed above for assistance. There is no charge to place or lift a security freeze.

Remain Vigilant and Lookout for Phishing Schemes. We also encourage you to remain vigilant in managing and handling your personal information and be on the lookout for suspicious emails, such as phishing schemes. Phishing schemes are attempts by criminals to steal personal information, including credit card numbers and social security numbers, over email. These attempts are often made by manipulating an email to make it look as if it came from a legitimate source, but which are actually sent by a fraudulent impersonator. Pay particular attention to anyone asking you to click on a link or attachment, especially if the email requests sensitive information, and pay close attention to

the email address (e.g., look for misspellings). It is also important that you check the recipient's email address when replying to emails to ensure it is legitimate. Also consider taking steps such as carrying only essential documents with you, being aware of how and with whom you are sharing your personal information, and shredding receipts, statements, and other sensitive information once you no longer need them.

For New York Residents: You may also obtain information about preventing and avoiding identity theft from the New York Attorney General's Office or New York's Office of Information Technology Services:

New York Attorney General's Office
Office of the Attorney General
The Capitol
Albany, NY 12224-0341
1-800-771-7755
https://ag.ny.gov/

New York Office of Information Technology Services
Empire State Plaza
P.O. Box 2062
Albany, NY 12220-0062
844-891-1786
https://its.ny.gov/