February 10, 2026

BY E- MAIL

New Hampshire Consumer Protection and Antitrust Bureau
Office of the Attorney General
33 Capital Street
Concord, NH 03301
DOJ-CPB@doj.nh.gov

To Whom It May Concern:

Managed Care Advisors/Sedgwick Government Solutions ("MCA/SGS") is providing this notice of a cybersecurity event to your office. MCA/SGS is a federal government contractor that provides federal agencies with workers' compensation and managed care solutions. MCA/SGS also manages the Nationwide Provider Network for the World Trade Center ("WTC") Health Program, which provides covered services for 9/11 responders and survivors with WTC-related illnesses.

On December 4, 2025, MCA/SGS discovered that files on a corporate Secure File Transfer Protocol ("SFTP") server were unexpectedly encrypted, as a result of unauthorized third party access to the server. MCA/SGS immediately initiated its incident response process. The company's investigation determined that the server was compromised on November 16, 2025 by an unauthorized third party. The affected SFTP server was immediately quarantined, all connections were disabled, and on December 5, 2025, a secure backup of the system was restored.

As of January 15, 2026, MCA/SGS has determined that approximately 3 residents of New Hampshire were affected. Depending on the individual, the types of affected data may have included: first name, last name, address, Social Security Number, date of birth, and Protected Health Information. On January 2, 2026, a ransomware group identifying itself as "TridentLocker" claimed credit for the incident and released approximately 3.4 GB of data associated with the SFTP server on a data leak site.

MCA/SGS will begin sending notifications to affected individuals on February 11, 2026. Attached is a copy of the consumer notification mailed to the affected individuals in your state. MCA/SGS is providing affected individuals with 12 months of complimentary credit monitoring and identity theft protection services through Kroll. We have also established a dedicated call center to answer individuals' questions.

We are working closely with a leading incident response firm, Mandiant, who is conducting a forensic analysis, and we also notified the FBI. Our current findings indicate that the incident was caused by a vulnerability in the SFTP application and was limited to the files within the SFTP server. We have also taken, and will continue to take, measures to protect our systems and data, including enhancing privacy protections in place with the relevant federal agency partners.

If you have any questions, please contact me at michael.smith@sedgwickgovernment.com.

Regards,

Michael Smith

Michael Smith
Chief Information Officer, & Chief Information Security Officer
Managed Care Advisors/Sedgwick Government Solutions

Enclosure

WTC Health Program Nationwide Provider Network

<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>

SCAN TO ENROLL

<<Date>> (Format: Month Day, Year)

NOTICE OF DATA BREACH

Dear <<First_name>> <<Last_name>>,

We are writing to inform you about a recent data privacy incident experienced by Managed Care Advisors/Sedgwick Government Solutions (MCA/SGS) that involved certain protected health information (PHI) associated with your World Trade Center (WTC) Health Program Nationwide Provider Network (NPN) member information. We are providing you with information about the incident and tools you can use to protect yourself against possible identity theft or fraud.

What Happened?

On December 4, 2025, we discovered that an unauthorized third party accessed a corporate server and encrypted some files. MCA/SGS initiated its incident response process and notified the WTC Health Program. Our investigation determined that the server was compromised on November 16, 2025, and that the activity was associated with an unauthorized third party.

The affected server was located outside the network where current member information resides. Our primary systems remain secure. The server was immediately quarantined, all connections were disabled, and on December 5th, a secure backup of the system was restored.

What Information Was Involved?

Your disclosed information contained files from the previous NPN contractor that may have included:

- Name
- Address
- Partial or full Social Security Number
- Medical record images
- Completed WTC Health Program Forms

What Are We Doing?

We are working closely with the WTC Health Program and a leading incident response firm, Mandiant, who is conducting a forensic analysis, and we also notified the Federal Bureau of Investigation (FBI). Our current findings indicate that the incident was caused by a vulnerability in the server application and was limited to the identified files. We will continue to work with our staff and the WTC Health Program to strengthen the privacy protections we have in place.

While we are not aware of identity theft or fraud related to information affected by this incident, as an additional precaution, we are offering you access to 12 months of complimentary credit monitoring and identity restoration services through Kroll at no charge to you.

Details about this offer and instructions on how to activate these services are enclosed with this letter. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation deadline)>> to activate your identity monitoring services.

Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

What Can You Do?

To help protect yourself from the possibility of identity theft, we recommend you enroll in the credit monitoring and identity restoration services by <<b2b_text_6 (activation deadline)>> and monitor your credit information for any signs of fraud or suspicious activity. If you notice any suspicious activity, we suggest you visit the Federal Trade Commission's Identity Theft protection website, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft.

For More Information

We sincerely apologize for the concern and inconvenience this incident may have caused. Your privacy is very important to us. If there is anything we can do to assist you, please call us at 1-844-425-7438 Monday through Friday, between the hours of 8 AM and 5:30 PM Central Time, excluding major U.S. holidays.

Sincerely,

Managed Care Advisors

Michael Smith

Michael Smith
Privacy Compliance Officer

Steps You Can Take to Help Protect Personal Information

Fraud Alerts: Consumers are entitled to one free credit report annually from each of the three major credit reporting bureaus: Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call 1-877-322-8228 toll-free. Consumers also have the right to place a free fraud alert on their credit file. An initial fraud alert lasts one year, and businesses are required to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you can place an extended fraud alert that lasts seven years. To place a fraud alert, contact any of the three nationwide credit reporting bureaus:

- **Equifax**: https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf
  - Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069
- **Experian**: https://www.experian.com/help/fraud-alert/
  - Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013
- **TransUnion**: https://www.transunion.com/fraud-alerts
  - TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016

Credit Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in a consumer's name without consent. Consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information: (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 they are a victim of identity theft. Should consumers wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

- **Equifax**: https://www.equifax.com/personal/credit-report-services/credit-freeze; 1-888-298-0045
  - Equifax Credit Freeze, P.O. Box 105788, Atlanta, GA 30348-5069
- **Experian**: https://www.experian.com/freeze/center.html; 1-888-397-3742
  - Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013
- **TransUnion**: https://www.transunion.com/credit-freeze; 1-800-916-8800
  - TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Federal Trade Commission: Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the three major credit reporting bureaus, the Federal Trade Commission, or your state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338). The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state attorney general. This notice has not been delayed by law enforcement.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement, including local law enforcement or the Iowa Attorney General. The Iowa Attorney General may be contacted at 1305 E. Walnut Street, Des Moines, IA 50319; 1-515-281-5926 or 1-888-777-4590 (outside of the Des Moines metro area); and www.iowaattorneygeneral.gov.

For Maryland residents: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, http://www.marylandattorneygeneral.gov, 1-888-743-0023.

For Massachusetts residents: Under Massachusetts law, individuals have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699 9001, http://www.ncdoj.gov/, 1-877-566-7226 to contact other nationwide consumer reporting agencies and to make freeze requests and obtain information on combating identity theft.

For New York residents: You may consider placing a Security Freeze on your credit report. For more information on a Security Freeze or on how to avoid identity theft, contact the New York Department of State Division of Consumer Protection (www.dos.ny.gov/consumer-protection; 1-800-697-1220) or the New York State Office of the Attorney General (www.ag.ny.gov; 1-800-771-7755).

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General. The Oregon Attorney General may be contacted at 1162 Court St. NE Salem, OR 97301-4096; 1-877-877-9392; and https://www.doj.state.or.us/oregon-department-of-justice/contact-us//. For more information about placing a security freeze, you can visit the Oregon Department of Justice Consumer Protection website at www.doj.state.or.us/consumer-protection/id-theft-data-breaches/identity-theft.

For Rhode Island Residents: For more information on how to prevent identity theft, you may contact the Rhode Island Attorney General at 150 South Main Street, Providence, RI 02903, 1-401-274-4400, and www.riag.ri.gov. You have the right to obtain a police report about this incident. There is approximately 1 Rhode Island resident that may be impacted by this event.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.