



Aubrey L. Weaver
Constangy, Brooks, Smith & Prophete, LLP
Cybersecurity & Data Privacy Team
1650 Market Street, Suite 3600
Philadelphia, PA 19103
AWeaver@constangy.com
941.875.5335

April 10, 2025

VIA ONLINE SUBMISSION

Attorney General Mike Hilgers
Office of the Attorney General
Consumer Protection Division
2115 State Capital
Lincoln, NE 68509
Email: ago.consumer@nebraska.gov

Re: Notice of Data Security Incident

Dear Attorney General Hilgers:

Constangy, Brooks, Smith & Prophete, LLP, represents Cabot Medical Care, an internal medicine and family medical provider located in Arkansas. CMC takes the protection of all information within its possession very seriously and has taken measures to reduce the likelihood of a similar incident reoccurring. The purpose of this letter is to notify you of the incident in accordance with Nebraska's data breach notification statute.

1. Nature of the Security Incident

On January 26, 2025, CMC became aware of unusual activity that disrupted access to certain systems. Upon discovering this activity, CMC immediately took steps to secure its network and launched an investigation with the assistance of independent cybersecurity experts to determine what happened. Through the investigation, it was revealed that certain information was acquired without authorization on January 26, 2025. Following this confirmation, CMC commenced a comprehensive review of the potentially affected data and worked diligently to obtain contact information to effectuate notification to potentially affected individuals, which process concluded on March 28, 2025.

The potentially affected information varies for each individual, but may have included individuals' names, Social Security numbers, and medical information.

2. Number of Nebraska Residents Affected

CMC notified five (5) Nebraska residents within the potentially affected population in accordance with Nebraska's data breach notification statute on April 9, 2025, via USPS First-Class Mail. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

3. Steps Taken Relating to the Incident

In response to the incident, CMC retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. CMC also implemented additional security measures to further harden its digital environment in an effort to prevent a similar event from occurring in the future.

CMC is also providing individuals with information about steps that they can take to help protect their personal information. Additionally, the notification letters provide twelve (12) months of complimentary identity protection services to each eligible individual whose Social Security number or driver's license information was potentially affected by this event, including credit and dark web monitoring, a \$1 million identity theft insurance policy, and fully managed identity theft recovery services. Those services are offered through Cyberscout, a company specializing in fraud assistance and remediation services. A call center will also be supported by Cyberscout for ninety (90) days to answer questions pertaining to the incident.

4. Contact Information

If you have any questions or need additional information, please do not hesitate to contact me at 215.770.4234 or aweaver@constangy.com.

Sincerely,

A handwritten signature in black ink, appearing to read 'Aubrey L. Weaver', with a stylized, flowing script.

Aubrey L. Weaver
Partner, Constangy Cyber Team

Attachment: Sample Notification Letter

Cabot Medical Care
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



April 9, 2025

Subject: Notice of Data Security Incident

Dear 

I am writing to inform you of a recent data security incident that may have affected your personal or protected health information. Cabot Medical Care (“CMC”) takes the privacy and security of all information within its possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your information.

What Happened. On January 26, 2025, CMC experienced a network disruption and immediately initiated an investigation of the matter. CMC engaged independent cybersecurity experts to assist with the process. As a result of the investigation, CMC determined that certain files may have been accessed and acquired without authorization on February 3, 2025. We then undertook a comprehensive review of those files and, in March 2025, learned that some of your personal information was contained within the potentially affected data which is the reason for this notification.

What Information Was Involved. The information may have included your name, date of birth, Social Security number, diagnosis or treatment information, and/or other health-related information.

What We Are Doing. As soon as CMC discovered this incident, CMC took the steps described above and implemented measures to enhance security and minimize the risk of a similar incident occurring in the future.

Additionally, to help relieve concerns and to help protect your information following this incident, CMC is providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve (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. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation 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:



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.

000010102G0500

P

What You Can Do. You can follow the recommendations on the following page to help protect your information. You can also enroll in the complementary services offered to you through Cyberscout by using the enrollment code provided above.

For More Information. Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call 1-833-998-8995 Monday through Friday from 8:00 am to 8:00 pm Eastern Time, excluding holidays. We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience this may cause.

Sincerely,

Cabot Medical Care
2037 West Main Street
Cabot, AR 72023

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 credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. 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 (the “FTC”).

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 www.annualcreditreport.com, calling toll-free 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
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 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. 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. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This 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. 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.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
www.marylandattorneygeneral.gov/Pages/CPD
888-743-0023

Oregon Attorney General
1162 Court St., NE
Salem, OR 97301
www.doj.state.or.us/consumer-protection
877-877-9392

California Attorney General
1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

New York Attorney General
The Capitol
Albany, NY 12224
800-771-7755
ag.ny.gov

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
www.riag.ri.gov
401-274-4400



00001020280000

P

Iowa Attorney General
1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

NY Bureau of Internet and Technology
28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

Washington D.C. Attorney
General
400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-protection
202-442-9828

Kentucky Attorney General
700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

NC Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers/
877-566-7226

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.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include 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; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit:

www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.