

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

JASON M. GOODWIN
jgoodwin@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, Pennsylvania 19422

Visit us online at
www.C-WLAW.com

NICHOLAS MARTIN
nmartin@c-wlaw.com

Telephone: (610) 567-0700
Fax: (610) 567-0712

March 7, 2025

Via Email (ag@riag.ri.gov)

Rhode Island Office of the Attorney General
150 South Main Street
Providence, Rhode Island 02903

RE: Data Incident Notification

To Whom It May Concern:

We serve as counsel for Community Care Alliance (“CCA”) located at P.O. Box 1700, Woonsocket, RI 02895. We write to provide notification of a recent data security incident. By providing this notice, CCA does not waive any rights or defenses under Rhode Island law, including the data breach notification statute.

On July 6, 2024, CCA experienced a network disruption that affected their ability to access certain systems. Upon discovery, CCA took immediate steps to respond and secure their network and systems, including the engagement of third-party forensic specialists to assist in a thorough investigation into the nature and scope of the incident. The investigation revealed that certain parts of the network may have been acquired by an unauthorized actor between July 1, 2024 and July 5, 2024. CCA immediately worked to review its systems to determine the types of information at risk and to whom it relates. On or around January 8, 2025, this process was completed and CCA worked to identify up-to-date contact information to provide individuals with notification.

On March 6, 2025, CCA received its results from a National Change of Address search and identified approximately 94,210 Rhode Island residents potentially affected by this incident. The information potentially impacted included first and last name, address, date of birth, driver's license number, Social Security number, diagnosis/condition, patient ID number, lab results, medications, health insurance information, provider name and/or other treatment information.

In response to this incident, CCA took steps to secure their environment, conducted an investigation, implemented additional technical measures, and notified law enforcement. Additionally, CCA began providing direct notice to the potentially impacted individuals on March 7, 2025 via U.S. mail. A copy of the notice is attached as **Exhibit A**. In an abundance of caution, CCA is offering the potentially impacted individuals complimentary credit monitoring and identity protection services.

Very truly yours,

CIPRIANI & WERNER, P.C.

By:


Jason M. Goodwin, Esq.

Exhibit A

Community Care Alliance
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



<Name>
<Address>



March 11, 2025

Dear <Name>:

Community Care Alliance writes to notify you about a recent data security incident we experienced that may have involved your data as outlined below. We take the privacy of information in our care very seriously and are providing you information about the incident, our response, and steps you can take to further protect your information should you feel it is necessary to do so.

What Happened: On July 6, 2024, we experienced a network disruption that affected our ability to access certain systems. Upon learning of this, we immediately began a comprehensive response and investigation with the support of third-party specialists. Through the investigation, we learned certain information may have been accessed or acquired by an unauthorized individual between July 1, 2024 and July 5, 2024. Upon discovery, we worked to identify the scope of data potentially at risk to perform a thorough review to identify the types of information potentially affected and to whom it relates. On or around January 8, 2025, this process was completed, and it was determined that your information may have been at risk. We then worked to identify up-to-date contact information to provide you with this notice as soon as possible.

What Information Was Involved: The types of information potentially at risk may have included your first and last name, in combination with one or more of the following data elements: address, date of birth, driver's license number, Social Security number, diagnosis/condition, lab results, medications, patient ID number, health insurance information, provider name and/or other treatment information.

What We Are Doing: In response to this incident, we immediately engaged third-party specialists to assist in the incident response and to conduct a thorough investigation. As part of this process, we implemented additional technical safeguards to further enhance the security of data we maintain and to prevent something similar from happening in the future. As an added precaution, we are making credit monitoring and identity protection services available to you for twelve (12) months at no cost to you.

What You Can Do: We recommend that you remain vigilant for potential incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for errors or suspicious activity. If you discover any suspicious or unusual activity on your accounts, please promptly contact the financial institution or company. We have provided additional information below, which contains more information about steps you can take to help protect yourself against fraud and identity theft should you feel it appropriate to do so.

For More Information: Should you have any questions or concerns, please contact our dedicated assistance line at 1- 833-998-5800 Monday through Friday, 8 a.m. to 8 p.m. Eastern Time (excluding major U.S. holidays). Community Care Alliance may also be contacted by mail at P.O. Box 1700, Woonsocket, RI 02895.

Sincerely,

Community Care Alliance

000010102G0500

2

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

How do I enroll for the free services?

In response to the incident, we are 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. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the 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.

To enroll in Credit Monitoring services at no charge, please log on to **www.mytrueidentity.com** and follow the instructions provided. When prompted please provide the following unique code to receive services: <Code>.

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 and explanation of benefits forms for suspicious activity and to detect errors. 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 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. If you have questions or notice incorrect information, contact the credit reporting bureau.

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.

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 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 fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000 TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian 1-888-397-3742 www.experian.com Experian Fraud Alert P.O. Box 9554 Allen, TX 75013 Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax 1-888-298-0045 www.equifax.com Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788
---	---	--



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 95,052 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>.