

March 25, 2022

Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Via Email

Attorney General Brian E. Frosh
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Data security Incident Involving CDI Health, LLC.

Dear Attorney General Frosh,

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents CDI Health, LLC. (“CDI Health”), a dialysis service provider which partners with Skilled Nursing Facilities and Hospital Services, located at 1717 W. 6th St., Suite 350, Austin, Texas 78703, with respect to a recent data security incident that was first discovered by CDI Health on March 4, 2022 (hereinafter, the “Incident”). CDI Health takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of Maryland residents being notified, and the steps that CDI Health has taken in response to the Incident. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring services.

Please note that the information contained herein is deemed to be confidential, non-public, and privileged. By sharing this information with your Office, CDI Health does not intend to waive any such confidentiality or privilege that may attach. CDI Health respectfully requests that your Office designate and treat this information as confidential and refrain from sharing this information with any third parties. CDI Health trusts the confidential information contained in this response demonstrates that CDI Health has taken prompt and effective action to address this incident.

1. Nature of the Incident

CDI Health discovered that an authorized party removed records from a secure location on March 4, 2022. CDI Health does not permit that any records that may contain sensitive personal information be removed from their secure location, so when it became aware of this Incident we immediately interviewed the party to discover why these records were removed.

After the conclusion of the internal investigation while CDI Health has no reason to believe that any individual information has been misused, CDI Health has determined that this removal of records potentially jeopardized the security of sensitive information.

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Alabama • Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston
Indiana • Kentucky • Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Mississippi • Missouri • Nashville • New Jersey • New Orleans
New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com

2. Number of Maryland residents affected.

CDI Health identified and has notified 44 individuals potentially affected by this Incident. Of those, one (1) was a resident of Maryland. Notification letters to these individuals were mailed on March 25, 2022, by first class mail. A sample copy of the March 25, 2022 notification letter is included with this letter under **Exhibit A**.

3. Steps taken in response to the Incident.

CDI Health values the privacy of the information it has within its control and will continue to do everything it can to protect it. CDI Health has taken the following steps: Inventoried all paper documents required in accordance with local, state, and federal laws and regulations associated with personnel files, secured all said documents in a locked cabinet and limited access to only the Arizona Regional Director, shredded all I9 documents and associated proof of identification, placed a digital copy in a secure digital file with access limited to CDI Health Human Resources, contracted with a secure, reputable digital company platform to move to paperless personnel files within the next three to six months, and retrained staff on document security, retention, and destruction in accordance with PHI & HIPAA guidelines.

Out of an abundance of caution, CDI Health is also providing individuals with 12 months of complimentary credit monitoring services through CyberScout at no charge to them.

4. Contact information

CDI Health remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Anjali C. Das

EXHIBIT A



[REDACTED]
[REDACTED]
[REDACTED]

March 25, 2022

Via First-Class Mail

Re: NOTICE OF DATA SECURITY INCIDENT

[REDACTED]

Out of an abundance of caution, CDI Health, LLC. ("CDI Health"), is writing to inform you of a data security incident that may have resulted in an unauthorized access of your personal information. CDI Health sincerely apologizes for this incident and any inconvenience it may cause you. While we are unaware of any fraudulent misuse of your personal information at this time, we are providing you with details about the events, steps that CDI Health is taking in response, and resources available to help you protect against the potential misuse of your information.

Why Do We Have Your Information?

CDI Health has your information because you are currently or were previously employed by CDI Health.

What Happened?

CDI Health discovered that an authorized party removed records from a secure location on March 4, 2022. CDI Health does not permit that any records that may contain sensitive personal information be removed from their secure location, so when it became aware of this Incident we immediately interviewed the party to discover why these records were removed.

After the conclusion of the internal investigation while CDI Health has no reason to believe that any individual information has been misused, CDI Health has determined that this removal of records potentially jeopardized the security of your sensitive information. Upon this discovery, CDI Health has decided to make notification to you, and to provide credit monitoring services to protect you from the potential misuse of personal data.

What Information Was Involved?

The personal information that may have been accessed by an unauthorized includes your name, as well as your: Name, Address, DOB, SS #, Passport #, DL #, Health information.

Please note that CDI Health has received no indication that your information has been used by the

unauthorized actor or by any unauthorized party to commit fraud. CDI Health is providing notice to you out of an abundance of caution.

What We Are Doing

CDI Health values the privacy of your information and will continue to do everything it can to protect it. CDI Health has taken the following steps: Inventoried all paper documents required in accordance with local, state, and federal laws and regulations associated with personnel files, secured all said documents in a locked cabinet and limited access to only the Arizona Regional Director, shredded all 19 documents and associated proof of identification, placed a digital copy in a secure digital file with access limited to CDI Health Human Resources, contracted with a secure, reputable digital company platform to move to paperless personnel files within the next three to six months, and retrained staff on document security, retention, and destruction in accordance with PHI & HIPAA guidelines.

Out of an abundance of caution, CDI Health is also providing you with 12 months of complimentary credit monitoring services through Cyberscout at no charge to you. While CDI Health is covering the cost of these services, you will need to complete the activation process by following the instructions enclosed to this letter.

What You Can Do

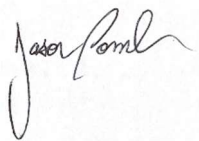
You may activate the credit monitoring services we are making available to you. Once again, CDI Health is making these services available to you at no cost; however, you will need to activate yourself in these services. **The deadline to enroll is June 26, 2022.** CDI Health would like to reiterate that, at this time, there is no evidence that your information was misused. However, CDI Health encourages you to take full advantage of the services offered.

Enclosed with this letter you will find additional information regarding the resources available to you, and the steps that you can take to further protect your personal information. CDI Health encourages you to enroll in the services offered and to remain vigilant against incidents of identity theft and fraud. Such vigilance includes reviewing account statements and credit reports for suspicious activity. Individuals are encouraged to report any suspicious activity to the affiliated institutions immediately.

For More Information:

The protection of your information is a top priority, and CDI Health, LLC sincerely regrets any concern or inconvenience that this matter may cause. If you have any questions, please do not hesitate to call the toll free number 1-800-405-6108, Monday through Friday, between 8:00 a.m. and 8:00 p.m. ET, excluding holidays. Representatives are available for 90 days.

Sincerely,



Jason Combs
President and CEO
CDI Health, LLC

Credit Monitoring

CDI Health is providing you with access to the following services:

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday. Please call the help line 1-800-405-6108 and supply the fraud specialist with your unique code listed below. To extend these services, enrollment in the monitoring services described below is required.

Additionally, we are providing you with access to **Single Bureau Credit Monitoring*** services at no charge. These services provide you with alerts for twelve months from the date of enrollment when changes occur to your Experian credit file. This notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event you become a victim of identity theft. These services will be provided by Cyberscout, a company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring* services at no charge, please log on to <https://www.myidmanager.com> 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 an email account, and services may not be available to minors under the age of 18 years of age. When signing up for monitoring services, you may be asked to verify personal information for our own protection to confirm your identity.

Steps You Can Take to Help Protect Your Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Furthermore, to help protect your deceased family member, there are steps you can take to request a copy of your deceased family member's credit report. An executor or surviving spouse can place a request to any of the three credit reporting agencies for a copy of the deceased individual's credit report. An executor or surviving spouse can also request that the following two notices be placed on a deceased individual's credit report:

- "Deceased – Do not issue credit"; or
- "If an application is made for credit, please notify the following person(s) (e.g. surviving relative, executor/trustee of the estate and/or local law enforcement agency – notifying the relationship)."

Contact information for the three nationwide credit reporting companies is as follows:

Equifax
PO Box 740241
Atlanta, GA 30374
www.equifax.com
1-800-525-6285

Experian
PO Box 9554
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion
PO Box 6790
Fullerton, CA 92834
www.transunion.com
1-800-680-7289

For more information regarding identity theft and the deceased, please visit <http://www.idtheftcenter.org> and search for “FS 117 - Identity Theft and the Deceased - Prevention and Victim Tips.” You should also notify the Social Security Administration and Internal Revenue Service of the death of your family member and that you received this letter.

Security 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 your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 https://www.equifax.com/personal/credit-report-services/credit-freeze/	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	TransUnion Security Freeze P.O. Box 160 Woodlyn, PA 19094 1-800-909-8872 www.transunion.com/credit-freeze
---	---	--

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (<https://www.transunion.com/fraud-alerts>); or
- Experian (<https://www.experian.com/fraud/center.html>).

A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact

information listed above. 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.

For residents of Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Colorado, Illinois, Iowa, Maryland, Missouri, New Mexico, North Carolina, Oregon, and West Virginia: It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a 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.

For residents of New Mexico: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach.

For residents of Oregon: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Rhode Island: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island: You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

District of Columbia Office of the Attorney General – Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General - 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - Consumer Protection Division: 200 St. Paul Place, 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

New York Office of Attorney General - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; <https://ag.ny.gov/consumer-frauds/identity-theft>

North Carolina Office of the Attorney General - Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226; www.ncdoj.com

Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence RI 02903; 1-401-274-4400; www.riag.ri.gov