



Martin McElligott
312.821.6219 (direct)
martin.mcelligott@wilsonelser.com

March 11, 2025

Via Online Portal

Attorney General Mike Hilgers
Office of the Attorney General
Consumer Affairs Response Team
2115 State Capitol
Lincoln, NE 68509

Re: Notice of Data Incident

Dear Attorney General Hilgers:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents Health Dimensions Group (“HDG”), a healthcare consulting and management company located at 12900 Whitewater Drive, Suite 201, Minneapolis, Minnesota, with respect to a recent cybersecurity incident (hereinafter, the “Incident”). This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of Nebraska residents being notified, and the steps that HDG has taken in response to the Incident. We have also enclosed hereto a sample of the notice letter mailed to the potentially impacted individuals, which includes an offer for complimentary credit monitoring services.

1. Nature of the Incident

On October 20, 2025, HDG became aware of a potential cybersecurity event involving its computer systems. Upon discovering the incident, HDG immediately activated its incident response plan and promptly engaged a third-party cybersecurity firm to secure its environment and investigate the cause and scope of the incident. On November 6, 2025, the ongoing investigation found evidence that HDG files were obtained by an unauthorized user. Based on this finding, HDG initiated a comprehensive review of the impacted data to determine what types of information, and which individuals may have been affected. On February 4, 2026, HDG’s review found evidence that personal information relating to its independent contractors was potentially impacted. HDG’s review remains ongoing to determine whether any additional individuals have been impacted as a result of the incident.

161 N Clark, Suite 4500 | Chicago, IL 60601 | p 312.704.0550 | f 312.704.1522 | wilsonelser.com

Albany, NY | Atlanta, GA | Austin, TX | Baltimore, MD | Birmingham, AL | Boston, MA | Charlotte, NC | Chicago, IL | Dallas, TX | Denver, CO | Detroit, MI | Long Island, NY
Hartford, CT | Houston, TX | Indianapolis, IN | Jackson, MS | Las Vegas, NV | London, England | Los Angeles, CA | Louisville, KY | Madison, NJ | McLean, VA | Merrillville, IN
Miami, FL | Milwaukee, WI | Nashville, TN | New Orleans, LA | New York, NY | Orange County, CA | Orlando, FL | Philadelphia, PA | Phoenix, AZ | Portland, OR | Raleigh, NC
San Diego, CA | San Francisco, CA | Sarasota, FL | Seattle, WA | Stamford, CT | St. Louis, MO | Tyler, TX | Washington, DC | West Palm Beach, FL | White Plains, NY

Although HDG is unaware of any fraudulent misuse of information, it is possible that the independent contractors' name, address and Social Security may have been exposed as a result of this unauthorized activity. As of this writing, HDG has not received any reports of related identity theft since the date of the incident (November 6, 2025, to present).

2. Number of Nebraska residents affected.

Based on the investigation conducted to date, HDG identified and notified three (3) Nebraska residents whose information may have been impacted as a result of the Incident. Notification letters to these individuals were mailed on March 11, 2026, by U.S. First Class Mail. A sample copy of the notification letter is included with this letter under **Exhibit A**.

3. Steps taken in response to the Incident.

HDG is committed to ensuring the security and privacy of all personal information in its control and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, HDG moved quickly to investigate and respond to the Incident, assessed the security of its systems, and notified individuals determined to be affected. Further, HDG implemented additional technical and administrative security measures to prevent a similar incident from occurring in the future.

Although HDG is not aware of any actual or attempted misuse of the affected personal information, HDG offered twelve (12) months of complimentary credit monitoring and identity theft restoration services through Cyberscout, a TransUnion company, to Nebraska residents to help protect their identity. Additionally, HDG provided guidance on how to better protect against identity theft and fraud, including providing information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and the contact details for the Federal Trade Commission.

4. Contact information

HDG remains dedicated to protecting the sensitive information within its control. Should you have any questions or need additional information, please do not hesitate to contact me at martin.mcelligott@wilsonelser.com or 312-821-6219.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Martin McElligott

EXHIBIT A

Health Dimensions Group
c/o Cyberscout
PO Box 245
Bellmawr, NJ 08099



March 11, 2026

Notice of Data Security Incident

Dear [REDACTED]

Health Dimensions Group (“HDG”) values and respects the privacy of your personal information, which is why we are notifying you of a recent incident that may have involved some of your personal information. Below you will find information about what happened, steps we are taking in response to the incident, and additional guidance to help you protect against information misuse.

What Happened?

On October 20, 2025, we became aware of a potential cybersecurity event involving its computer systems. Upon discovering the incident, we immediately activated our incident response plan and promptly engaged a third-party cybersecurity firm to secure its environment and investigate the cause and scope of the incident. On November 6, 2025, the ongoing investigation found evidence that HDG files were obtained by an unauthorized user. Based on this finding, we initiated a comprehensive review of the impacted data to determine what types of information, and which individuals may have been affected. On February 4, 2026, our review found that personal information relating to independent contractors was potentially impacted.

While we have not received any reports of information being misused as a result of the incident, we are notifying you for purposes of full transparency.

What Information Was Involved?

Based on our investigation, the following information was potentially subject to unauthorized access: name, Social Security number.

What We Are Doing

Data privacy and security is among HDG’s highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information within our care. Since discovery of the unauthorized activity, we moved quickly to investigate the incident, confirm the security of its systems, and notify affected individuals. Additionally, we implemented additional data security measures and will continue to take steps to mitigate the risk of future harm.

We are also 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 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 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.

What You Can Do

To enroll in Credit Monitoring services at no charge, please log on to [REDACTED] 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 ninety (90) days from the date of this letter. Enrollment requires an internet connection and e-mail account and may not be available to minors under the age of eighteen (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.

Additionally, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. You can find more information on steps to protect your personal information in the enclosed *ADDITIONAL RESOURCES TO HELP PROTECT YOUR INFORMATION* sheet.

For More Information

We value the trust you place in us and sincerely regret any concern or inconvenience this matter may cause. Rest assured we remain dedicated to ensuring the privacy and security of all information in our control. Should you have any questions not addressed in this letter or need assistance enrolling in credit monitoring, please call [REDACTED] (toll free) during the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday (excluding U.S. national holidays).

Sincerely,

Amber Rogotzke, President
Health Dimensions Group

ADDITIONAL RESOURCES TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts We recommend that you remain vigilant for incidents of fraud or identity theft by regularly reviewing your credit reports and financial accounts for any suspicious activity. You should contact the reporting agency using the phone number on the credit report if you find any inaccuracies with your information or if you do not recognize any of the account activity.

You may obtain a free copy of your credit report by visiting www.annualcreditreport.com, calling toll-free at 1-877-3228228, or by mailing a completed Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report for a fee by contacting one or more of the three national credit reporting agencies.

You have rights under the federal Fair Credit Reporting Act (FCRA). The FCRA governs the collection and use of information about you that is reported by consumer reporting agencies. You can obtain additional information about your rights under the FCRA by visiting <https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act>.

Credit Freeze You have the right to add, temporarily lift and remove a credit freeze, also known as a security freeze, on your credit report at no cost. A credit freeze prevents all third parties, such as credit lenders or other companies, whose use is not exempt under law, from accessing your credit file without your consent. If you have a freeze, you must remove or temporarily lift it to apply for credit. Spouses can request freezes for each other as long as they pass authentication. You can also request a freeze for someone if you have a valid Power of Attorney. If you are a parent/guardian/representative you can request a freeze for a minor 15 and younger. To add a security freeze on your credit report you must make a separate request to each of the three national consumer reporting agencies by phone, online, or by mail by following the instructions found at their websites (see “Contact Information” below). The following information must be included when requesting a security freeze: (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth (month, day, and year); (iv) current address and any previous addresses for the past five (5) years; (v) proof of current address (such as a copy of a government-issued identification card, a recent utility or telephone bill, or bank or insurance statement); and (vi) other personal information as required by the applicable credit reporting agency.

Fraud Alert You have the right to add, extend, or remove a fraud alert on your credit file at no cost. A fraud alert is a statement that is added to your credit file that will notify potential credit grantors that you may be or have been a victim of identity theft. Before they extend credit, they should use reasonable procedures to verify your identity. Please note that, unlike a credit freeze, a fraud alert only notifies lenders to verify your identity before extending new credit, but it does not block access to your credit report. Fraud alerts are free to add and are valid for one year. Victims of identity theft can obtain an extended fraud alert for seven years. You can add a fraud alert by sending your request to any one of the three national reporting agencies by phone, online, or by mail by following the instructions found at their websites (see “Contact Information” below). The agency you contact will then contact the other credit agencies.

Federal Trade Commission For more information about credit freezes and fraud alerts and other steps you can take to protect yourself against identity theft, you can contact the Federal Trade Commission (FTC) 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 should also report instances of known or suspected identity theft to local law enforcement and the Attorney General’s office in your home state and you have the right to file a police report and obtain a copy of your police report.

Contact Information Below is the contact information for the three national credit reporting agencies (Experian, Equifax, and TransUnion) if you would like to add a fraud alert or credit freeze to your credit report.

Credit Reporting Agency	Access Your Credit Report	Add a Fraud Alert	Add a Security Freeze
Experian	P.O. Box 2002 Allen, TX 75013-9701 1-866-200-6020 www.experian.com	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 https://www.experian.com/fraud/center.html	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/freeze/center.html
Equifax	P.O. Box 740241 Atlanta, GA 30374-0241 1-866-349-5191 www.equifax.com	P.O. Box 105069 Atlanta, GA 30348-5069 1-800-525-6285 www.equifax.com/personal/credit-report-services/credit-fraud-alerts	P.O. Box 105788 Atlanta, GA 30348-5788 1-888-298-0045 www.equifax.com/personal/credit-report-services
TransUnion	P.O. Box 1000 Chester, PA 19016-1000 1-800-888-4213 www.transunion.com	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-alerts	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

Iowa and Oregon residents are advised to report suspected incidents of identity theft to local law enforcement, to their respective Attorney General, and the FTC.

Massachusetts residents are advised of their right to obtain a police report in connection with this incident.

District of Columbia residents are advised of their right to obtain a security freeze free of charge and can obtain information about steps to take to avoid identity theft by contacting the FTC (contact information provided above) and the Office of the Attorney General for the District of Columbia, Office of Consumer Protection, at 400 6th St. NW, Washington, D.C. 20001, by calling the Consumer Protection Hotline at (202) 442-9828, by visiting <https://oag.dc.gov>, or emailing at consumer.protection@dc.gov.

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

New York residents are advised that in response to this incident they can place a fraud alert or security freeze on their credit reports and may report any incidents of suspected identity theft to law enforcement, the FTC, the New York Attorney General, or local law enforcement. Additional information is available at the website of the New York Department of State Division of Consumer Protection at <https://dos.nysits.acsitefactory.com/consumerprotection>; by visiting the New York Attorney General at <https://ag.ny.gov> or by phone at 1-800-771-7755; or by contacting the FTC at www.ftc.gov/bcp/edu/microsites/idtheft/ or <https://www.identitytheft.gov/#/>.

North Carolina residents are advised to remain vigilant by reviewing account statements and monitoring free credit reports and may obtain information about preventing identity theft by contacting the FTC (contact information provided above) or the North Carolina Office of the Attorney General, Consumer Protection Division at 9001 Mail Service Center, Raleigh, NC 27699-9001, or visiting www.ncdoj.gov, or by phone at 1-877-5-NO-SCAM (1-877-566-7226) or (919) 7166000.

Rhode Island residents are advised that they may file or obtain a police report in connection with this incident and place a security freeze on their credit file and that fees may be required to be paid to the consumer reporting agencies.