

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

MEGHAN S. FARALLY
mfarally@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, Pennsylvania 19422

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

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

June 27, 2022

Via E-Mail (IDTheft@oag.state.md.us)

Office of the Attorney General
200 St. Paul Place
Baltimore, Maryland 21202

RE: Data Incident Notification

To Whom It May Concern:

We serve as counsel for Jordan Health Products, LLC d/b/a Avante Health Solutions ("Avante") located at 875 North Michigan Avenue, Chicago, Illinois 60610 and write to inform you of a recent data security incident. By providing this notice, Avante does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On May 12, 2022, Avante was victimized by a sophisticated ransomware attack that impacted its network. Upon discovery, Avante immediately took steps to secure the network and began an internal investigation. Further, Avante engaged third-party specialists to assist with a thorough, forensic investigation. On May 27, 2022, the investigation confirmed unauthorized access to the Avante network from May 5, 2022 through May 12, 2022. The investigation further determined that certain Avante data may have been subject to unauthorized access. Avante then immediately reviewed its internal files and compiled a list of individuals potentially impacted and worked to obtain sufficient address information in order to provide notification.

On June 14, 2022, the review was completed, and it was determined that information related to 18 Maryland residents was potentially subject to unauthorized access. While the investigation into the full nature and scope of this incident remains ongoing, the information believed to be at risk includes the first and last name of current employees, former employees, dependents, and beneficiaries, in combination with one or more of the following: Social Security number; U.S. alien registration number; passport number; driver's license or state issued ID number; military ID number; tax ID number; non-U.S. national identification number; account number; credit/debit card number; incidental health reference; medical treatment information/diagnosis; prescription information; provider name; MRN/patient ID; Medicare/Medicaid number; health insurance information; and/or treatment cost information.

On June 27, 2022, Avante sent written notice of this incident to the potentially impacted Maryland residents pursuant to Maryland state law. The notice letter included an offer of complimentary credit monitoring and identity protection services for twelve (12) months. The notice letter sent to individuals is substantially similar to the letter attached hereto as Exhibit "A."

Very truly yours,

A handwritten signature in blue ink, appearing to read "Meghan Farally". The signature is fluid and cursive, with the first name "Meghan" and last name "Farally" clearly distinguishable.

Meghan Farally, Esq.
CIPRIANI & WERNER, P.C.

Exhibit A

<<First Name>> <<Last Name>>

<<Address1>> <<Address2>>

<<City>>, <<State>> <<Zip>>

To Enroll, Please Call:

1-800-939-4170

Or Visit:

<https://app.idx.us/account-creation/protect>

Enrollment Code: <<XXXXXXXXXX>>

June 27, 2022

Dear <<First Name>> <<Middle Name>> <<Last Name>> <<Suffix>>:

We are writing to inform you of a cyber incident experienced by Avante Health Solutions ("Avante") that may have involved your information described below. The information believed to be at risk from this incident includes information related to current employees, former employees, their beneficiaries, and/or the family members of current and former employees who may have participated in Avante's health insurance plan. While we have no evidence of attempted or actual misuse of your information as a result of this incident, we are providing you with information about the incident, our response, and steps you can take to help protect your information.

What Happened:

On May 12, 2022, Avante was victimized by a sophisticated ransomware attack that impacted our network. Upon discovery, we immediately began working with our I.T. team and third-party computer specialists to conduct an investigation to determine how this incident occurred. While our investigation remains ongoing, we have discovered that certain Avante current and former employee data, kept in the normal course of business, may have been subject to unauthorized access. Although we are unable to confirm the specific information that may be affected for each individual at this time, we are providing notification in an abundance of caution.

What Information Was Involved:

While our investigation into the full nature and scope of this incident remains ongoing, the information believed to be at risk may include your first and last name, in combination with one or more of the following: Social Security number; U.S. alien registration number; passport number; driver's license or state issued ID number; military ID number; tax ID number; non-U.S. national identification number; account number; credit/debit card number; incidental health reference; medical treatment information/diagnosis; prescription information; provider name; MRN/patient ID; Medicare/Medicaid number; health insurance information; and/or treatment cost information.

What We Are Doing:

Upon discovery, we immediately engaged third-party forensic specialists to investigate this matter. Out of an abundance of caution, we have arranged for you to activate, at no cost to you, an online credit monitoring service for <<12/24>> months provided by IDX. Due to privacy laws, we cannot activate these services for you directly. Additional information regarding how to activate the complimentary credit monitoring service is enclosed. We have also provided additional information about steps you can take to help protect yourself against fraud and identity theft.

What You Can Do:

We recommend that you remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your accounts, please promptly contact your financial institution or company. Additionally, you can enroll to receive the complimentary credit monitoring service we are making available to you. You can also review the enclosed "Steps You Can Take to Help Protect Your Information" for additional resources.

For More Information:

Should you have additional questions or concerns regarding this matter, please do not hesitate to contact us at 1-800-939-4170 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is September 27, 2022.

We take the privacy and security of the information in our care seriously, and sincerely regret any worry or inconvenience it may cause you and your family.

Sincerely,

A handwritten signature in black ink, appearing to read "Jim Leidl", written in a cursive style.

Jim Leidl
President & COO

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever 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 some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

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
---	---	--

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

ADDITIONAL ACTIONS TO HELP PROTECT YOUR 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. This notice has not been delayed by law enforcement.

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 www.oag.state.md.us. Avante Health Solutions may be contacted at 875 North Michigan Avenue, Chicago, IL 60610.

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 [#] Rhode Island residents impacted by this incident.

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 441 4th Street NW #1100, Washington, D.C. 20001; 202-727-3400, and <https://oag.dc.gov/consumer-protection>. Avante Health Solutions may be contacted at 875 North Michigan Avenue, Chicago, IL 60610.