WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

July 20, 2023

Via Certified Mail; Return Receipt Requested

RECEIVED
JUL 25 2023
CONSUMER PROTECTION

Attorney General John Formella
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301
attorneygenral@doj.nh.gov

Re: Virtual Private Network Solutions, LLC d/b/a VPN Solutions, LLC ("VPN") Ransom Attack

Dear Attorney General Formella:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Associates in Dermatology ("AID"), with respect to a ransom attack that Virtual Private Network Solutions, LLC d/b/a VPN Solutions, LLC ("VPN") experienced.

This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of New Hampshire residents being notified, and the steps that AID 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.

1. Nature of the Incident

On or around October 31, 2021, **VPN experienced a ransomware**. VPN informed AID on December 22, 2021 that none of AID's data hosted on VPN was impacted by this incident, however a forensics investigation was still ongoing. On March 30, 2022, AID was informed again by VPN that none of AID data was impacted by the incident. AID followed up many times to receive a formal report of what information was impacted. On January 17, 2023, VPN informed AID that on or about November 15, 2022, they identified files pertaining to AID that potentially contained sensitive information. VPN determined that these files are tag image files from a data warehouse, **not an electronic medical record system**, the majority of which do not contain personally identifiable information and/or protected health information. VPN was able to match some files to patient names, but did not confirm if these files contained protected health information nor did VPN's list fully identify the names of individuals and the type of data that may have been compromised by the ransom attack.

AID has been working to identify all the specific individuals and the type of data that was impacted by VPN's breach in order to provide sufficient notice. AID has no reason to believe that any individual's information has been misused as a result of this event.

The types of information that was identified by VPN as compromised varied with each individual. Data elements may include one or more of the following types of information:

Please note that not all information was impacted for each individual.

2. Number of New Hampshire residents affected.

A total of two (2) New Hampshire residents may have been potentially affected by this incident. A notification letter to these individuals were mailed by first class mail on July 19, 2023. A sample copy of the notification letter is included with this letter under **Exhibit A**.

3. Steps taken in response to the Incident.

Based on VPN's correspondence with us, VPN has represented to us the following: VPN's forensic investigation efforts to date have not been able to determine the cause or origin of the incident, including whether the incident may have been the result of access through a third-party system. Following the incident, VPN began building an entirely new environment to host its data including robust security controls and endpoint detection and response solution. VPN completed rebuilding its entire environment and restoring all data. VPN continues to maintain multiple endpoint detection and response solutions in the new environment with the use of Sentinel One and Carbon Black EDR and is continuing to work to identify and implement measures to further strengthen the security of its systems to help prevent this from happening in the future.

AID has performed a review of its contracts with third party vendors and their cybersecurity environment. AID also offered of complimentary credit monitoring and identity theft restoration services through CyberScout to the potentially impacted individuals to help protect their identity. Additionally, AID 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

Associates in Dermatology remains dedicated to protecting the sensitive information that is hosted by its third party vendors. If you have any questions or need additional information, please do not hesitate to contact my colleague,

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das

EXHIBIT A

Associates in Dermatology
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB-07296 1-1

ASSOCIATES DERMATOLOGY

Via First-Class Mail

[redacted]

July 19, 2023

Re: Notice of Cybersecurity Incident

Dear [redacted],

Virtual Private Network Solutions, LLC d/b/a VPN Solutions, LLC ("VPN") provides electronic health record management services to health care providers. Associates in Dermatology ("AID") uses VPN's software, TouchChart, where VPN hosts AID patient information. This notice is intended to alert potentially impacted individuals of a data breach incident VPN experienced, steps we are taking in response, and resources available to assist and protect individuals.

What Happened? On or around October 31, 2021, **VPN experienced a ransomware**. VPN informed AID on December 22, 2021 that none of AID's data hosted on VPN was impacted by this incident, however a forensics investigation was still ongoing. AID followed up many times to receive a formal report of what information was impacted. On January 17, 2023, VPN informed AID that on or about November 15, 2022, they identified files pertaining to AID that potentially contained sensitive information. VPN determined that these files are tag image files from a data warehouse, **not an electronic medical record system**, the majority of which do not contain personally identifiable information and/or protected health information. VPN was able to match some files to patient names, but did not confirm if these files contained protected health information nor did VPN's list fully identify the names of individuals and the type of data that may have been compromised by the ransom attack. On March 10, 2023, AID determined that the compromised files may have also contained personally identifiable information.

AID is working to identify all the specific individuals and the type of data that was impacted by VPN's breach in order to provide sufficient notice. On June 2, 2023, AID determined that you were impacted by this incident and obtained your mailing address to provide you notice. AID has no reason to believe that any individual's information has been misused as a result of this event.

What Information Was Involved? While we have no reason to believe that information has been misused as a result of this incident, we are notifying you for purposes of full transparency. The types of information that was identified by VPN as compromised varied with each individual. Based on a review our review, the unauthorized party may have had access to:

What VPN Is Doing: Based on VPN's correspondence with us, VPN has represented to us the following: VPN's forensic investigation efforts to date have not been able to determine the cause or origin of the incident, including whether the incident may have been the result of access through a third-party system. Following the incident, VPN began building an entirely new environment to host its data including robust security controls and endpoint detection and response solution. VPN completed rebuilding its entire environment and restoring all data. VPN continues to maintain multiple endpoint detection and response

solutions in the new environment with the use of Sentinel One and Carbon Black EDR and is continuing to work to identify and implement measures to further strengthen the security of its systems to help prevent this from happening in the future.

What We Are Doing: Data privacy and security is among AID's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care. In response to the incident, AID has performed a review of its contracts with third party vendors and their cybersecurity environment.

AID is 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 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 through Identity Force, a TransUnion company specializing in fraud assistance and remediation services. While we are covering the cost of these services, you will need to complete the activation process by following the instructions below.

What You Can Do: 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. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

To enroll in Credit Monitoring services at no charge, please log on to 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 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.

We would like to reiterate that, at this time, there is no evidence that your information was misused. However, we encourage you to take full advantage of the services offered.

For More Information

For individuals seeking more information or questions about this incident, please call AID's dedicated toll-free helpline at between the hours of 8:00 am to 8:00 pm Eastern Time, Monday through Friday.

Once again, Associates in Dermatology sincerely apologizes for any inconvenience this incident may cause, and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Charlie McCall
Chief Financial Officer
Associates in Dermatology

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.

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

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-800-525-6285
www.experian.com/fraud/center.html	www.transunion.com/fraud-alerts	https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

Security Freeze: You 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:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-888-298-0045
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	https://www.equifax.com/personal/credit-report-services/credit-freeze/

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. Instances of known or suspected identity theft should also be reported to law enforcement.

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. 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, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; 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 at www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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